Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2016

Jami Roininen

TIETOTURVATYÖPAJOJEN HYÖDYNTÄMINEN YRITYKSEN TIETOTURVAKEHITYKSESSÄ

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

2016 | 71 sivua + 4 liitettä

Jarkko Paavola

Jami Roininen

TIETOTURVATYÖPAJOJEN HYÖDYNTÄMINEN YRITYKSEN TIETOTURVAKEHITYKSESSÄ

Henkilöstön tietoturvallisen toiminnan kehittämiseksi ja tietoturvatietoisuuden lisäämiseksi toimeksiantaja käynnisti tietoturvatietoisuuskampanjan. Kampanjan yksi merkittävä vaihe oli tietoturvatyöpajatyöskentely. Tämän vaiheen tehokkaaseen ja kattavaan hyödyntämiseen perehdyttiin tässä opinnäytetyössä. Tavoitteena oli työpajoja järjestämällä kehittää lääkealalla toimivan kohdeyrityksen Suomessa työskentelevän henkilöstön tietoturvatietoisuutta ja -osaamista. Lisäksi tarkoituksena oli kartoittaa työntekijöiden toiminnan tietoturvallisuuden parannuskohteita ja laatia tietoturvan kehitysehdotuksia henkilöstön toimintaa ajatellen. Osallistujamäärälle asetettiin oma alitavoitteensa. Työpajoihin kutsuttiin kaiken kaikkiaan 523 työntekijää, joista 80 % oli tavoitteena saada osallistumaan.

Tavoitteiden saavuttamiseksi järjestettiin työpajoja, joita hyödynnettiin mahdollisimman kattavasti. Tämä tarkoitti sitä, että työpajoja käytettiin koulutustilaisuuksina, joissa pyrittiin lisäämään osallistuvan henkilöstön tietoturvatietoisuutta ja -osaamista. Lisäksi henkilöstön toiminnan tietoturvallisuudessa olevia parannuskohteita kerättiin avoimen kyselylomakkeen avulla. Kaksisivuinen kyselylomake toimi samalla myös harjoitteena työpajatilaisuuksissa.

Kaiken kaikkiaan 48 järjestettyyn työpajaan osallistui 84 % kutsutusta henkilöstöstä eli yhteensä 440 työntekijää. Suurin osa osallistuneista työntekijöistä koki, että järjestetyt työpajat lisäsivät heidän tietoturvatietoisuuttaan. Valtaosa osallistujista pitivät työpajoja myös hyödyllisinä ajatellen osastojen tietoturvallisen toiminnan lisäämistä. Merkittävimpänä havaintona voidaan pitää sitä, että kohdeyrityksen henkilöstöllä on tietoturvan kannalta runsaasti parannettavaa omassa toiminnassaan.

Tietoturvatyöpajat osoittautuivat tehokkaaksi menetelmäksi kouluttaa työntekijöitä ja kartoittaa heidän toimintansa parannuskohteita tietoturvallisuutta ajatellen. Työpajatyöskentely oli miellyttävä tapa käsitellä tietoturva-aiheita, joita ei aina pidetä mielekkäinä työntekijöiden keskuudessa. Kattavien tulosten avulla yritys pystyy tekemään jatkotoimenpiteitä sekä etenemään henkilöstön ja monialaisen kokonaistietoturvan kehittämisessä.

ASIASANAT:

Henkilöstö, kehittäminen, tietoturva, tietoturvatietoisuus, työpaja.

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2016 | 71 pages + 4 appendices

Jarkko Paavola

Jami Roininen

UTILIZATION OF INFORMATION SECURITY WORKSHOPS IN A COMPANY'S INFORMATION SECURITY DEVELOPMENT

The commissioning company, which is a large company in the area of pharmaceutical industry, launched an information security awareness campaign. The objectives of this campaign were to increase the personnel's information security awareness and to direct their behavior to a more secure direction. One of the most important and concrete methods used to carry out this campaign was group working in information security workshops. In this thesis these workshops and the efficient utilization of them are described. The first objective of this thesis was to increase information security awareness and skills of the commissioning company's personnel with information security workshops. Identifying the examples of the personnel's non-secure behavior and creating a list of improvement suggestions were also the main objectives of this thesis. In total 523 employees were invited to these workshops. The target participation rate, which is 80 percent, was additionally considered as an objective.

To reach all objectives, these information security workshops would be used as training events in which participants would be trained to increase their information security awareness and skills. In addition, examples of the personnel's non-secure behavior, which needs to be improved, would be collected with an open questionnaire. The two-paged open questionnaire form would also serve as an information security exercise to all participants.

In total, 48 workshops were arranged and attended by 440 employees, which are 84 percent of all invited employees. The majority of participants agreed that the workshops increased their information security awareness. Most of them also considered the workshops useful to enhance their department's information security awareness. One of the most significant observations from these workshops was the fact that the company's personnel have to improve many aspects of their information security behaviour.

The information security workshops turned out to be a very effective method to train personnel and find examples of non-secure behavior. Working in small groups was a comfortable way to go through information security topics which are usually not considered as the most delightful topics among personnel. With the help of these comprehensive results, the company can consider and implement the next steps to increase its overall information security level.

KEYWORDS:

Development, information security, information security awareness, personnel, workshop.

SISÄLTÖ

LIITTEET

KUVAT

KUVIOT

TAULUKOT

1 JOHDANTO

Yritysten arvokkaat tiedot ja etenkin liikesalaisuudet herättävät kiinnostusta ulkopuolisissa tahoissa. Tietoturvarikollisuuden uhka on aina läsnä ja tiedon tehokas turvaaminen on tärkeämpää kuin koskaan aikaisemmin. Fyysinen suoja, tietoturvapolitiikat ja -säännöt sekä pääsyoikeuksien rajoitukset auttavat yrityksiä nostamaan omaa tietoturvatasoaan. Riittävää tietoturvatasoa ei kuitenkaan voida saavuttaa ilman turvallisesti toimivaa henkilöstöä. Organisaatiot kouluttavat ja arvioivat henkilökuntaansa sekä korostavat tietoturvatietoisuuden merkitystä koko yrityksen tietoturvan edistämisessä. Korkea tietoturvataso auttaa varmistamaan liiketoiminnan menestymisen ja tekee yrityksestä luotettavan toimijan.

Tässä opinnäytetyössä tutkimuksen kohteena on erään lääkeyrityksen henkilöstön tietoturvallisuus. Tutkimus suoritetaan toimeksiannon pohjalta. Opinnäytetyön tavoitteina on työpajoja järjestämällä lisätä kohdeyrityksen lähes koko Suomen henkilöstön tietoturvatietoisuutta ja -osaamista sekä kartoittaa henkilöstön toiminnan tietoturvallisuuden kriittisimmät kehityskohteet. Havaintojen perusteella suositellaan lisäksi seuraavia askeleita tietoturvatason kehittämiseksi. Toimeksiantajalle on tärkeää, että työpajatyöskentelyä hyödynnetään mahdollisimman kattavasti. Tämän vuoksi kouluttamisen lisäksi työpajoista kerätään runsaasti tutkimusaineistoa erityisesti henkilöstön tietoturvallisen toiminnan parannuskohteiden kartoittamiseksi. Työpajat ovat osa yrityksen globaalia tietoturvakampanjaa, joka käynnistettiin kasvavan tiedon ja tietoturvauhkien määrän vuoksi.

Opinnäytetyön kohdeyritys eli toimeksiantaja on kansainvälinen lääkealan suuryritys. Yrityksellä on toimintaa ympäri maailmaa ja yrityksen Suomen toiminnan roolia pidetään merkittävänä. Normaaliin liiketoimintaan liittyy lukuisia tietoturvahaasteita, joista yksi on henkilöstön tietoturvallinen toiminta. Yrityksen pääasiallinen toiminta on keskittynyt Suomessa kahteen toimipisteeseen, jotka sijaitsevat Espoossa ja Turussa. Muu toiminta hoidetaan etätyönä esimerkiksi kotitoimistoilla tai erilaisissa markkinointitapahtumissa. Yrityksen henkilöstöön kuuluu Suomessa kaiken kaikkiaan noin 820 henkilöä. Turun toimipisteessä tuotannon tehtävissä työskentelee noin 300 henkilöä ja toimihenkilöitä on yli 350. Espoossa yrityksen nimissä työskentelee 110 henkeä sekä vuokratyöntekijöinä ja palveluntoimittajina 60 henkilöä.

Varsinaisia tutkimustehtäviä opinnäytetyössä on kolme. Ensimmäinen tutkimustehtävä muodostuu henkilöstön kouluttamisesta tietoturvatyöpajoja järjestämällä. Toinen tutkimustehtävä muodostuu kerätyn tutkimusaineiston kokoamisesta tuloksiksi ja kolmas tutkimustehtävä puolestaan suositusten listaamisesta tietoturvakehityksen ja käyttäytymismuutoksen tueksi. Opinnäytteen on tarkoitus toimia henkilöstöä koskevan tietoturvan kehittämisvälineenä, jota kohdeyritys voi valitsemallaan tavalla hyödyntää omissa jatkotoimenpiteissään.

Tehtävän tutkimuksen on tarkoitus olla sekä kartoittava että kuvaileva tutkimus. Tutkimuksen päätutkimusotteena käytetään kvantitatiiviseen eli määrälliseen tutkimukseen painottuvaa tutkimusotetta. Merkittävä osa tutkimusta on henkilöstön toiminnan kehittäminen, joten tutkimus on kvantitatiivisen tutkimuksen ohella myös toimintatutkimuksellinen. Tutkimuksen tutkimusmetodi on puolestaan survey-tutkimus, jossa hyödynnetään myös tapaustutkimukselle tyypillisiä havainnointimenetelmiä. Survey-tutkimus eli suomeksi kyselytutkimus suoritetaan avoimin kyselylomakkein, joiden avulla saadaan kohdeyrityksen henkilöstöltä vapaamuotoisia ja vaihtelevia vastauksia.

Opinnäytetyön teoreettisessa osassa käsitellään tiedon, tietoturvan ja sen kehittämisen teoriaa keskittyen pääasiassa ihmiseen ja yrityshenkilöstöön. Lähdemateriaalina käytetään laajasti tietoturvakirjallisuutta ja verkkolähteitä. Opinnäytteen empiirisessä osassa esitellään tietoturvatyöpajat järjestelyineen sekä analysoidaan niiden tuloksia. Tulosten pohjalta pohditaan suosituksia yrityksen tietoturvallisuuden tason nostamiseksi henkilöstön osalta. Opinnäytteen liitteiksi on lisätty listat työpajoihin osallistuvista osastoista ja tutkimusaineiston keräämiseksi käytetyt työarkit.

2 TIETO JA TIETOTURVA

2.1 Tieto tietoturvan yhteydessä

Termejä ”tieto”, ”informaatio” ja ”data” käytetään suomen kielessä usein sekaisin ja myös toistensa synonyymeinä. Etenkin tiedosta puhuttaessa saatetaan käyttää myös termiä ”informaatio”. Näiden termien eroavaisuudet ja yhteydet on kuitenkin hahmotettava väärinkäsitysten välttämiseksi. Data ja informaatiota voidaan yksinkertaisimmillaan jaotella siten, että tietokoneet tarvitsevat dataa ja ihmiset tietoa. (Doyle 2014.) Monen muun teoksen ja dokumentin tapaan tässä opinnäytetyössä käytetään tietoturvan yhteydessä yleisellä tasolla termiä ”tieto”, koska suomen kielessä on haastavaa antaa tiedolle tai informaatiolle yhtä selkeää merkitystä.

Tarkemmin tarkasteltuna data on viittauksia tai analyysejä varten kerätty fakta- ja tilastokokoelma. Tietotekniikan yhteydessä dataa ilmaistaan lukumäärinä, merkkeinä tai symboleina, joiden toimintaa tietokoneet hallinnoivat. Dataa kuljetetaan ja tallennetaan elektronisten signaalien muodossa. Mikäli dataa halutaan tallentaa, se tehdään magneettiselle, optiselle tai mekaaniselle tallennusmedialle. (Iyengar 2010, 49.) Esimerkkejä magneettisista tallennusmedioista ovat kiintolevyt, optisista CD-levyt (Compact Disk) ja mekaanisista vanhat reiälliset paperikortit.

Data on täysin merkityksetöntä ilman asiayhteyttä. Merkitys muodostuu vasta, kun data-arvot yhdistetään johonkin tiettyyn asetteluun tai olosuhteeseen. Esimerkiksi data-arvo 20 on merkityksetön ilman asiayhteyttä. Arvosta tulee kuitenkin merkityksellinen ja käytännöllinen, jos sille annetaan asiayhteydeksi esimerkiksi mitta. Senttimetreinä luku 20 kertoo paljon enemmän kuin pelkkä arvo 20. Kun data on yhdistetty asiayhteyteen, se muuttuu informaatioksi. (Copley 2015.)

Informaatio muodostuu tietotekniikan eli IT:n (Information Technology) yhteydessä datasta, joka on viety tiettyyn muotoon ja tiettyä tarkoitusta varten. Tietokoneohjelmat voivat esimerkiksi käyttää data-arvoja syötetietoina ja antaa tietokoneen näyttöruudulle tulokset sekä tulosteet tietona selkeästi luettavassa muodossa. (Iyengar 2010, 49.)

Tallennettu data on saatavilla joko fyysisinä kopioina, kuten paperidokumentteina tai täysin elektronisessa muodossa. Fyysisiä kopioita säilytetään esimerkiksi laatikoissa, kaapeissa ja varastoissa. Elektronista dataa säilytetään puolestaan esimerkiksi

tietokannoissa ja tiedostohakemistoissa. Datan säilytystavasta riippumatta se on hyvin altis haavoittuvuuksille. Siksi dataa on suojeltava vaurioilta, varkaudelta sekä datan eheyden menettämiseltä. (Iyengar 2010, 49.)

Datasta tulee siis informaatiota, joka myöhemmin voi päätyä ihmisen hyödynnettäväksi tiedon muodossa. Tiedon turvaamisesta muodostuu lähtökohtaisesti tietoturvallisuuden ja lyhyemmin tietoturvan käsite.

2.2 Tietoturvan määritelmä

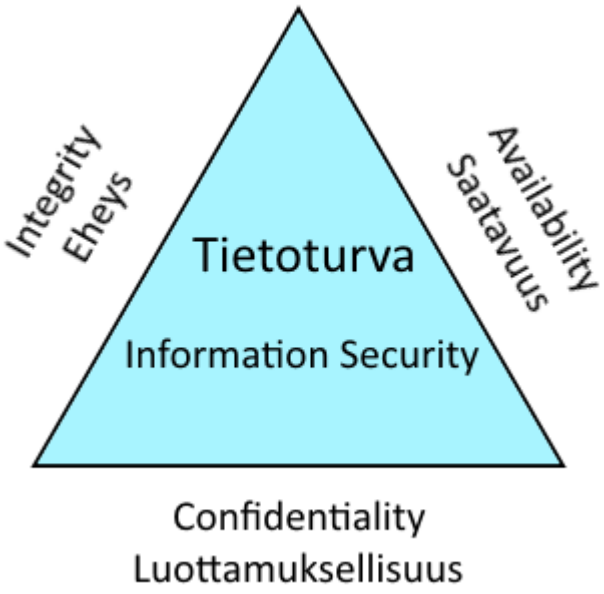
Tietoturva muodostuu käsitteenä CIA-triadin (Confidentiality, Integrity and Availability Triad) tavoitteellisista perusperiaatteista sekä kiistämättömyydestä, todentamisesta ja pääsynvalvonnasta. Tietoturvallisuuden tarkemmat tavoitteet ovat tietojen, järjestelmien, palveluiden sekä tietoliikenteen suojaaminen normaali- ja poikkeusoloissa. Näiden tavoitteiden saavuttamiseksi toimeenpannaan hallinnollisia, teknisiä sekä muita mahdollisesti tarvittavia toimenpiteitä. (Väistö 2005, 2.)

Tietoturva tai tietoturvallisuus tarjoaa keinoja ja toimintamalleja tietosuojan ylläpitämiseen. Tietoturva ja tietosuoja ovat sanamuodoltaan hyvin samanlaiset, ja niillä on joitain yhtäläisyyksiä. Lopulliselta merkitykseltään ne ovat kuitenkin täysin eri asioita, eikä termejä tule sekoittaa toisiinsa. Tietosuoja tarkoittaa erityisesti ihmisten itsemääräämisoikeuden ja yksityisyyden suojaamista. Heikko tietoturvataso johtaa siihen, että tietosuojan avulla suojattavan tiedon suojaamisesta tulee vaikeaa. Tämän takia tietosuojan ja tietoturvan yhteydet on tärkeä ymmärtää ja hahmottaa tietoturvasta puhuttaessa. (Laaksonen ym. 2006, 17.)

2.2.1 CIA-triadi

Tietoturva voidaan jakaa käsitteen laajuuden takia kolmeen tavoitteelliseen periaatteeseen. Nämä periaatteet ovat tiedon luottamuksellisuuden, eheyden ja saatavuuden takaaminen. (Rousku 2014, 47.) Periaatteet muodostavat yhdessä CIA-triadin. CIA-triadilla tarkoitetaan tunnettua kolmiomallia, jolla voidaan tunnistaa tietoturvan ongelma-alueet sekä tarpeelliset ratkaisut näillä alueilla. (Perrin 2008.) Triadin etuliitteen lyhenne CIA muodostuu englanninkielisistä sanoista ”Confidentiality”, ”Integrity” ja ”Availability”. Suomeksi käännettynä sanat ovat järjestyksessä jo esille

tulleet luottamuksellisuus, eheys ja saatavuus. CIA-triadin kolmiorakenne on esitetty Kuviossa 1.



Kuvio 1. CIA-triadi.

Luottamuksellisuudella tarkoitetaan tiedon suojaamista luvattomalta pääsyltä. Luottamuksellisuuden toteutumisen varmistamiseksi on toimittava siten, että vain ennalta valituilla henkilöillä on pääsy tietoon. Näille henkilöille on siis harkitusti myönnetty oikeus päästä käsiksi tiettyihin tietoihin. Yksinkertainen esimerkki luottamuksellisuudesta muodostuu tietokoneella olevan tiedoston pääsyoikeuksien rajaamisesta. Tällä tavalla ne henkilöt, joiden ei haluta pääsevän käsiksi tiedostoon, eivät enää omaa pääsyoikeutta siihen. Tähän tiedostoon pääsevät käsiksi kuitenkin ne henkilöt, joille pääsyoikeus on myönnetty. (Henderson 2015.)

Eheys merkitsee etenkin datan suojaamista ei-halutuilta muutoksilta ja sen hävittämiseltä. On kuitenkin mahdollista, että datan muuttamiseen oikeutettujen henkilöiden tekemät muutokset aiheuttavat vahinkoa datalle. Tämän takia on varmistettava, että mahdolliset vahingot voidaan korjata. Mikäli tämä varmistus on kunnossa, pystytään takaamaan datan eheyden säilyminen. (Perrin 2008.)

Tiedon saatavuudella tarkoitetaan yksinkertaisimmillaan sitä, että tiedon on oltava sitä tarvitsevan saatavilla. Tietoteknisissä palveluissa ja järjestelmissä olevaa tietoa saatetaan tavoitella käyttäjän toimesta mihin kellonaikaan tahansa. Tästä seuraavan ympärivuorokautisen saatavuuden takaaminen vaatii usein uutta teknologiaa ja aiheuttaa kuluja palveluntarjoajille. Tämä voi johtaa laiminlyönteihin ja palveluiden toimintaa häiritsevien verkkohyökkäysten onnistumiseen. (Rousku 2014, 50–51.)

Mikäli palveluissa on toimintakatkoksia, saatavuus kärsii välittömästi. Välttämättömät huoltotoimenpiteiden aiheuttamat katkokset ovat kuitenkin ymmärrettäviä ja yleisesti hyväksyttyjä. (Rousku 2014, 50.) Saatavuuden toteutumattomuus näkyy käytännössä esimerkiksi siten, että verkkosivustolle yhdistettäessä sivusto ei palvelun toiminta-ongelmista johtuen avaudukaan. Mikäli kyseiseltä sivustolta haluttaisiin lukea esimerkiksi uutisia, ei se tässä tapauksessa tule onnistumaan. Verkkoselaimeen avautuvan sivuston sijaan tietokoneen näyttöruudulle tulee vain ilmoitus, että sivusto ei ole käytettävissä tai sitä ei voida ladata.

Tunnetun CIA-triadin luottamuksellisuus, eheys ja saatavuus auttavat yhdessä hahmottamaan tietoturvan käsitettä. Kolmiomallia ei tule käyttää suoraan turvallisuuden tarkistuslistana. Mallia voidaan kuitenkin käyttää tietoturvallisuuden kehittämisen lähtökohtana esimerkiksi tietoturvapolitiikan laatimisessa. (Perrin 2008.)

2.2.2 Kiistämättömyys

Kiistämättömyydellä tarkoitetaan ominaisuutta, jolla todistetaan, että tietty tapahtuma tai toiminto on tapahtunut. Onnistuneen ja pitävän todistuksen myötä tapahtunutta ei voida kiistää jälkikäteen. (Commission for the Protection of Privacy 2015.)

Kiistämättömyyttä käytetään yleisesti esimerkiksi sähköpostiviestinnän yhteydessä. Sähköpostiviesteissä kiistämättömyys takaa sen, ettei vastaanottaja voi kieltää vastaanottaneensa viestiä. Lähettäjä ei puolestaan voi kieltää lähettäneensä viestiä. (Commission for the Protection of Privacy 2015.)

2.2.3 Todentaminen

Todentamisella eli autentikoinnilla tarkoitetaan osapuolten, henkilön tai järjestelmän luotettavaa tunnistamista. Todentamisella viitataan yleensä siihen, mitä kohteella on

hallussaan tai mitä kohde tietää. Todentamisen vahvuus voidaan varmistaa yhdistämällä nämä kaksi ominaisuutta. Kun nämä kaksi ominaisuutta yhdistetään, puhutaan vahvasta todentamisesta. (Opetushallitus 2012.)

Monet järjestelmät toteuttavat todentamisen yhteydessä myös tunnistamisen. Henkilön tiedot voidaan tarkistaa ajokortista tai passista, ja samalla suorittaa myös käyttäjän tunnistaminen. Järjestelmät, kuten kulunvalvontajärjestelmät voivat puolestaan valtuuttaa ja todentaa samaan aikaan. Kulunvalvontajärjestelmissä henkilön kulkukortti luetaan, ja ovi aukeaa saman tien, mikäli kulkukortin haltijalle on myönnetty kulkuoikeus kohteeseen. (Opetushallitus 2012.)

2.2.4 Tunnistaminen

Tunnistaminen on menettely, jossa käyttäjä tai järjestelmä yksilöidään. Tunnistaminen voi tapahtua ilman, että kohteen tarvitsee tehdä mitään toimenpiteitä. Tällöin tunnistaminen tapahtuu automaattisesti jonkun toisen henkilön tai järjestelmän toimesta. (Opetushallitus 2012.)

Yksinkertainen esimerkki tunnistamisesta on työpaikalla tapahtuva tunnistaminen. Työntekijän tunnistaminen tapahtuu tällöin toisten työntekijöiden toimesta. Työntekijät tunnistavat tutun työntekijän ja toteavat tämän työympäristöön kuuluvaksi. (Opetushallitus 2012.)

2.2.5 Pääsynvalvonta

Tietoteknisessä mielessä pääsynvalvonnalla säädellään sitä, kuka tai mikä pääsee katsomaan tai käyttämään resursseja tietoteknisissä ympäristöissä. Pääsynvalvonta voidaan jakaa fyysiseen ja loogiseen valvontaan. Fyysinen pääsynvalvonta rajoittaa pääsyä rakennuksiin, huoneisiin ja tietotekniseen omaisuuteen. Looginen pääsynvalvonta rajoittaa puolestaan yhteyksiä tietoverkkoihin sekä pääsyä järjestelmien tiedostoihin ja dataan. (Rouse 2014.)

Pääsynvalvonta jaetaan fyysisen ja loogisen valvonnan lisäksi neljään eri kategoriaan. Nämä kategoriat ovat Mandatory Access Control, Discretionary Access Control, Role Based Access Control ja Rule Based Access Control. (Techotopia 2009.)

Mandatory Access Control on tarkin pääsynvalvonnan muoto. Tässä mallissa pääsyä eri resursseihin kontrolloidaan käyttöjärjestelmien ja järjestelmänvalvojien määrittämien asetusten avulla. Resursseja voivat olla esimerkiksi tiedostot. Mandatory Access Control -mallissa käyttäjät eivät voi muuttaa pääsynvalvonta-asetuksia, vaan heidän oikeutensa rajoittuvat järjestelmissä ylläpidon määrittelemällä tavalla. (Techotopia 2009.)

Discretionary Access Control -mallissa jokaisella käyttäjällä on pääsyoikeus omaan dataansa. Tämän malli on tyypillisesti oletusarvona useimmissa käyttöjärjestelmissä. Discretionary Access Control -mallissa jokaisen objektin kanssa toimii Access Control -lista. Access Control -lista sisältää käyttäjät ja ryhmät, joille käyttäjä on myöntänyt pääsyoikeuden sekä näille myönnetyn pääsyoikeuden tason. Esimerkiksi käyttäjä A voi myöntää tekstitiedostoonsa vain lukuoikeuden käyttäjälle B sekä täydet luku- ja kirjoitusoikeudet ryhmälle 1. Tässä mallissa käyttäjä voi kuitenkin myöntää pääsyoikeuden vain niihin resursseihin, jotka hän jo valmiiksi omistaa. (Techotopia 2009.)

Role Based Access Control ja Rule Based Access Control ovat selkeitä pääsynvalvonnan malleja. Role Based Access Control perustuu siihen, että tietylle roolille organisaatiossa annetaan tietyt pääsyoikeudet. Tämän jälkeen käyttäjille annetaan omaan toimenkuvaan sopiva ja ennalta määritelty rooli. Rule Based Access Control perustuu puolestaan sääntöihin, jotka järjestelmänvalvoja määrittelee. Sääntöjen perusteella myönnetään tai estetään pääsy johonkin resurssiin. Rule Based Access Control käyttää myös Access Control -listoja pääsyn myöntämiseen. Kun käyttäjä tai ryhmä yrittää avata esimerkiksi tiedoston, käyttöjärjestelmä tarkastaa Access Control -listan säännöt tämän tiedoston osalta. (Techopedia 2009.)

2.3 Tietoturvan osa-alueet

Tietoturva voidaan jakaa eri osa-alueisiin. Jaottelut voivat olla erilaisia, mutta perinteisin jaottelu jakaa tietoturvan kahdeksaan eri alueeseen. (Andreasson & Koivisto 2013, 52.) Perinteisen jaottelun alueet ovat seuraavat:

- Hallinnollinen turvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus

- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus.

(Andreasson & Koivisto 2013, 53.)

2.3.1 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus on tietoturvallisuuden johtamistoiminto ja organisaation tietoturvatoiminnan lähtökohta. Organisaation johdon hyväksymät tietoturvaperiaatteet, vastuunjako, tietoturvaan satsattavat resurssit sekä riskiarviointi muodostavat yhdessä hallinnollisen turvallisuuden kokonaisuuden. Henkilöstöä koulutetaan, ohjeistetaan, valvotaan ja arvioidaan tietoturvallisten toimintamallien pohjalta. Nämä kaikki ovat välttämättömiä tietoturvallisuuden ylläpitämiseksi ja kehittämiseksi. (Väistö 2005, 4.)

Käyttäjien tulee ymmärtää ne periaatteet, jotka muodostavat organisaation tietoturvallisuuden ja sen muodollisen kehittämisen perustan. Tätä varten organisaation johto laatii tietoturvapolitiikan, joka asetetaan koko henkilökunnan saataville. Organisaation tietoturvaohjeistus ja -koulutus perustuvat tietoturvapolitiikassa määritettyihin suuntaa antaviin linjauksiin. Näillä linjauksilla johto osoittaa tukevansa turvallisuuden kehittämistä. Tietoturvapolitiikan sisältö eri linjauksineen riippuu organisaation johdon keskustelujen ja näkemysten perusteella laaditusta dokumentaatiosta. (Laaksonen ym. 2006, 146–148; Väistö 2009, 4.)

Politiikkaa laadittaessa ei ole suotavaa suoraan lainata valmiita malleja esimerkiksi toisesta yrityksestä tai organisaatiosta. Muiden mallit eivät välttämättä ole soveltuvia oman organisaation tietoturvatarpeisiin. Lisäksi omien mietintöjen ja keskustelujen pohjalta laadittuihin linjauksiin sitoudutaan paremmin kuin lainattuihin näkemyksiin. (Laaksonen ym. 2006, 148.)

Käyttäjiltä vaaditaan tietoturva-asioissa paljon, mutta johdon tulee selkeästi määrittää, kirjoittaa muistiin sekä kouluttaa ja ohjeistaa heidän vastuunsa. Tarkka johdon toiminta varmistaa sen, että käyttäjät pystyvät toimimaan vastuun edellyttämällä tavalla. (Väistö 2005, 4.)

2.3.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus on yksinkertaisesti henkilöstöstä aiheutuvien riskien hallintaa. Henkilöstöturvallisuus ja henkilöturvallisuus ovat termeinä lähellä toisiaan, mutta ne eivät kuitenkaan ole sama asia. Henkilöturvallisuudella tarkoitetaan henkilöihin kohdistuvien tietoturvariskien hallintaa. Tietoturvallisuuden yhteydessä henkilöstöturvallisuus tarkoittaa henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietojen ja tietojärjestelmien käytön yhteydessä. (Valtiovarainministeriö 2008a, 11–12.)

Henkilöstötietoturvallisuudella on keskeinen merkitys tietojen turvaamisessa, ja haasteita sille asettaa ihminen omalla toiminnallaan. Henkilöstö käsittelee omassa työssään valtavasti tietoa vastaanottamalla, muokkaamalla, tallentamalla, välittämällä ja tuhoamalla sitä. Työntekijöillä on myös oma keskeinen roolinsa organisaation tietojärjestelmien ja -varastojen ylläpidossa. (Valtiovarainministeriö 2008a, 12.)

Tietoa voidaan monistaa ja lähettää ilman, että alkuperäinen tieto katoaisi minnekään. Tarvittaessa tieto voidaan kuitenkin kadottaa helposti ja myös hävittää vahingossa. Tiedon hallitseminen on suuri haaste organisaatioiden toiminnalle, koska sitä on valtavat määrät sähköisessä ja paperisessa muodossa. Henkilöstöturvallisuus koskettaa jokaista organisaatiossa toimivaa henkilöä ja on erittäin keskeinen alue jokaisen organisaation tietoturvallisuudessa. (Valtiovarainministeriö 2008a, 12).

2.3.3 Fyysinen turvallisuus

Ihmisiä, tietoja, laitteita ja tiloja suojattaessa keskitytään fyysiseen turvallisuuteen. Lähtökohtaisesti tärkeimpänä pidetään ihmisten, kuten yrityksen työntekijöiden suojaamista. Laitteiden ja tietojen korvaaminen on helpompaa kuin yksittäisen henkilön, joka hallitsee oman työnsä kokonaisvaltaisesti ja tuntee yrityksen toimintatavat. Tietoja suojataan onnettomuuksilta ja katastrofeilta, jotta niitä ei menetettäisi. Laitteita ja tiloja, joissa tietoja säilytetään, tulee myös turvata. Siinä missä menetetyn työntekijän korvaaminen voi olla todella työlästä, laitteen hankinta tai tilan korjaaminen on usein helpompi toteuttaa. Se on yksi osasyy siihen, ettei laitteiden ja tilojen suojaamiseen panosteta yhtä paljon kuin henkilöiden fyysiseen suojaamiseen. (Andress 2011, 97–98.)

Fyysistä turvallisuutta uhkaavat monet eri tekijät. Nämä uhkatekijät voidaan jakaa seuraaviin luokkiin:

- Äärimmäiset lämpötilat
- Kaasut
- Nesteet
- Elävät organismit
- Sinkoilevat objektit ja kappaleet
- Objektien fyysinen liikehdintä
- Energiapoikkeamat
- Ihmiset
- Toksiinit
- Tuli ja savu.

(Andress 2011, 98.)

Äärimmäisen korkeat tai matalat lämpötilat voivat olla suuri uhka turvallisuudelle, jos niiden vaikutuksia ei huomioida. Tulipalot voivat aiheuttaa mittavaa tuhoa yritykselle ja tulipaloista seuraavat savut, kaasut sekä muut toksiinit ovat etenkin henkilöstölle suuri uhka. Tulipaloista tai muusta onnettomuudesta johtuvat räjähdykset ja niiden seurauksena sinkoilevat objektit voivat uhata sekä ihmisiä että laitteita ja tiloja. Veden kaltaiset nesteet saattavat aiheuttaa suurina määrinä vahinkoa tilarakenteisiin ja lopulta myös laitteet voivat kärsiä pahastikin. Energiatasojen poikkeamat, kuten voimakkaat elektroniset virrat ja kaikenlaiset fyysiset liikkeet voivat rikkoa laitteita tai jopa kokonaisia rakenteita. Elävät organismit eli eliöt ja ihmiset voivat myös uhata turvallisuutta omalla toiminnallaan.

2.3.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden tavoitteena on tiedonsiirtoyhteyksien täysi käytettävyys, tiedonsiirron suojaaminen ja salaaminen, käyttäjien vahva tunnistus ja tietoverkonverkon toiminnan varmistaminen ja valvominen. (Sosiaali- ja terveysministeriö 2007, 14.)

Tietoliikenneturvallisuus on suuri kokonaisuus, joka pitää sisällään tietoliikennelaitteiston ja sen luetteloinnin, ylläpitotoiminnan, muutosvalvonnan sekä -dokumentoinnin. Tietoliikenneverkkoja ja niissä tapahtuvaa viestintää tulee valvoa huolellisesti ja

varmistaa niiden hallittu toteutus. Kaikenlaiset poikkeamat verkon tapahtumissa pitää ottaa vakavasti ja dokumentoida oikein. Lisäksi tietoliikenneverkkoja ja -ohjelmia tulee testata aktiivisesti tietoturvapuutteiden löytämiseksi ja tietoliikenneturvallisuuden varmistamiseksi. (Sosiaali- ja terveysministeriö 2007, 29.)

2.3.5 Laitteistoturvallisuus

Laitteiden turvaamiseen ja niiden saatavuuteen keskittyvät toimenpiteet muodostavat laitteistoturvallisuuden kokonaisuuden. Laitteistoturvallisuudella turvataan ennen kaikkea tietoteknisten laitteistojen elinkaarta. Elinkaareen kuuluu kaikki laitteiston asennukset, takuut sekä ylläpidolliset toiminnot. Lisäksi elinkaari sisältää tuotetukipalvelut, niitä koskevat sopimukset ja lopulta laitteen turvallisen hävittämisen, kun se jää tarpeettomaksi tai menee rikki. (Valtiovarainministeriö 2008b, 57.)

Laitteistoturvallisuuden ollessa puutteellista yrityksen on esimerkiksi hankalaa pitää tietotekniset laitteet käyttäjien saatavilla. Mikäli yrityksellä ei ole omaa tietoteknistä ylläpitoa tai sopimuksia tuotetuesta, epäkunnossa olevista tärkeistä laitteista voi koitua suuriakin ongelmia liiketoiminnalle.

2.3.6 Ohjelmistoturvallisuus

Organisaation käytössä olevista ohjelmistoistakin tulee pitää hyvää huolta. Käyttöjärjestelmät, ohjelmistot ja sovellukset tulee suojata tunnistautumismenetelmin siten, etteivät ulkopuoliset pääse niihin käsiksi. Ohjelmistoturvallisuus kattaa suojauksen ja tunnistautumisen lisäksi myös ohjelmistojen valvonnan ja lokimenettelyt, joilla seurataan ohjelmistojen käyttöä ja niihin liittyviä tapahtumia. Päivittäinen ohjelmistojen ylläpito ja oikea-aikainen päivittäminen kuuluvat myös ohjelmistoturvallisuuteen. (Penttinen 2015, 16.)

Ohjelmistojen turvallisuus lähtee ohjelmiston kehitysvaiheesta. Kehityksessä ja ohjelmoinnissa käytetyt prosessit määrittävät ohjelmiston turvallisuuden lähtötason. Valmiiden ohjelmistojen ollessa käytössä tietoturvaan vaikuttavat myös sekä niiden omat asetusmääritykset että palvelualustan asetukset. Palvelualustoja ovat yleensä käyttöjärjestelmät ja niiden rinnalla toimii myös usein muita apuohjelmistoja. Asetusten ja teknisten asioiden lisäksi ohjelmistoturvallisuuteen liittyy myös ihminen. Käyttäjiä tulee

kouluttaa ja ohjeistaa kattavasti, jotta ohjelmistotietoturvallisuuden ja yleisen tietoturvan taso voidaan maksimoida. (Suomen Kuntaliitto, 2016.)

2.3.7 Tietoaineistoturvallisuus

Tietoaineistot, kuten asiakirjat, tiedostot, muut tiedot ja tietoa sisältävät järjestelmät, tulee olla organisaation kontrollissa. Tämä kontrolli pitää sisällään aineistojen tunnistuksen, luokittelun, säilyttämisen, hävittämisen ja valvonnan. (Valtionhallinnon tarkastusvirasto 2011, 16.)

Aineistot tulee tunnistaa, jotta voidaan olla varmoja niiden oikeellisuudesta. Erilaiset salassa pidettävät tietoaineistot luokitellaan organisaatioissa eri tavoin. Luokittelu voi koostua esimerkiksi täysin julkisesta tiedosta, organisaation sisäisestä tiedosta, rajoitetusta tiedosta ja todella salaisesta tiedosta. Tietoaineistoja tulee säilyttää siten, että niihin pääsevät käsiksi vain tarvittavat henkilöt. Säilyttämisen lisäksi aineistojen hävittäminen on hoidettava turvallisesti. Esimerkiksi luottamuksellisia asiakirjoja ei tule heittää tavalliseen paperinkeräykseen. Asiakirjat voivat jatkokäsittelyn yhteydessä joutua vääriin käsiin, eikä tähän pystytä enää yrityksen tai organisaatioin toimesta suoraan vaikuttamaan. Mikäli arkaluontoisen materiaalin valvotusta hävittämisestä on sovittu sopimuksin jätehuollon kanssa, voidaan toimintaa pitää lähtökohtaisesti turvallisena.

Tiivistetysti kaikkea luottamuksellisiin tietoaineistoihin liittyvää toimintaa tulee hallita oikein aina uuden aineiston luomisesta sen hävittämiseen asti. Tämä laaja tietoaineistojen kontrollointi on varsinkin isojen yritysten kohdalla merkittävä haaste suuren tietomäärän vuoksi.

2.3.8 Käyttöturvallisuus

Käyttöturvallisuus koostuu päivittäisistä menettelytavoista, joita organisaatio toteuttaa päivittäisessä työssään säilyttääkseen hyvän tietoturvatason. Käyttöturvallisuudessa merkittävässä asemassa ovat henkilöstön työkäytäntöjä koskevat periaatteet, salasanat sekä käytettävien ohjelmien hallittu käyttö. Työntekijälle tulee antaa vain tarvittavat oikeudet järjestelmiin ja tietoihin. Näin hän pystyy hoitamaan tarvittavat työtehtävät ja samalla minimoidaan väärinkäytösten tai vahinkojen mahdollisuus. Salasanoille tulee määrittää kriteerit, jotta ne ovat tarpeeksi monimutkaisia ja vaikeasti arvattavia.

Ohjelmien hallittu käyttö on myös erittäin tärkeää. Mikäli ohjelmistoja käytetään osaamisen puutteen takia väärin, saattavat vahingot olla yritykselle varsin merkittäviä. (Oikarinen 2012, 7; i&i Solutions 2015, 6.)

Tietoturvan eri osa-alueet ovat itsessäänkin suuria kokonaisuuksia ja yhdessä ne muodostavat tietoturvan käsitteen. Osa-alueet eroavat toisistaan, mutta niissä on myös yhtäläisyyksiä. Selkeitä rajanvetoja tietoturvan eri osa-alueiden välille ei voida vetää, vaan ne täydentävät toisiaan. Jokainen osa-alue on siksi otettava huomioon tietoturvaa rakennettaessa ja ylläpidettäessä. Tässä opinnäytetyössä keskitytään ihmiseen tietoturvan yksittäisenä lenkkinä ja toimijana. Siksi työn kannalta keskeisimpänä osa-alueena voidaan pitää henkilöstöturvallisuutta. Henkilöstöturvallisuuden ohessa on kuitenkin painotettava myös hallinnollisen turvallisuuden sekä käyttöturvallisuuden merkitystä.

3 HENKILÖSTÖ JA TIETOTURVA

Yrityksen työntekijöiden tärkein tehtävä on hoitaa ne työtehtävät, jotka heille on annettu. Päivittäiset työtehtävät tulee suorittaa tehokkaasti ja annettujen ohjeiden mukaisesti. Yrityksen taloudellinen menestys on tärkeä päämäärä, jota yritetään saavuttaa kaikin keinoin. Asetettuja päämääriä tavoitellaan usein myös tietoturvan kustannuksella. Keskityttäessä luomaan ja tuottamaan tehokkaasti tuotteita ja palveluita kiire, huolimattomuus ja piittaamattomuus voivat aiheuttaa mittavia vahinkoja yritykselle. Kun henkilöstölle asetetaan tavoitteita ja tuotantovaatimuksia, on huomioitava työntekijöiden rooli tietoturvassa.

Yrityksen työntekijä, yksittäinen ihminen on joko tietoturvan heikoin tai vahvin lenkki. Vaikka yrityksellä olisi käytössään viimeisintä turvallisuusteknologiaa tai ja yleisesti korkea suojataso, kouluttamaton henkilöstö voi johtaa suuriin ongelmiin. Käyttäjille voidaan antaa tietoturvasuunnitelman mukaisesti hyvät tunnistautumisvälineet tunnuksineen ja salasanoineen. Tunnukset tuovat mukanaan kuitenkin suuren vastuun, sillä näillä tunnuksilla voidaan päästä käsittelemään, jakamaan, tulostamaan, muuttamaan sekä tuhoamaan yrityksen tietoja. Tämän takia henkilöstön tietoturvaosaamiseen ja -tietoisuuden lisäämiseen tulee panostaa merkittävästi. (SANS Institute 2001, 8.)

3.1 Henkilöstön tietoturvatietoisuus

Henkilöstön tulee olla tietoinen tietoturvaan liittyvistä asioista ja ihmisten käyttäytymistä tulee ohjata tietoturvallisempaan suuntaan. Työntekijä voi päästä työssään käsiksi arkaluonteiseen tietoon ja siksi tulee huolehtia, että he toimivat tiedon arvon mukaisesti. Tietoturvatietoisuus on enemmän kuin vuotuisten tietoturvahiirimattojen – kuten perinteisten salasanaohjeita sisältävien mattojen – jakamista henkilöstölle. Siitä voidaan lähteä liikkeelle, mutta tietoturvakehityksen ei tule jäädä siihen. (McIlwraith 2012, 2.)

Henkilöstön kannustaminen vaikuttaa merkittävästi tietoturvatietoisuuden tasoon. Tietoturvatietoisuutta kehitettäessä pyritään tilanteeseen, jossa jokaisen työntekijän jokapäiväinen käyttäytyminen on täysin turvallista. Tämä on haasteellista, koska käyttäytymiseen vaikuttaa moni tekijä. Ihmisen käyttäytyminen perustuu päätöksiin, joita hän tekee omien tietojensa, kokemustensa ja ennakkoluulojensa perusteella. Päätöksiin

voi vaikuttaa myös psykologiset tekijät ja tilanne, jossa ratkaisu tulisi tehdä. Päätöksiä voidaan tehdä harkitsemattomasti ja nopeasti tai vaihtoehtoisesti vasta pitkänkin harkinnan jälkeen. (McIlwraith 2012, 3.)

Tietoturvatietoisuus on kriittinen osa yrityksen ja sen henkilöstön päivittäistä toimintaa. Monimutkaisimmissakin tietoteknisissä toteutuksissa ihmisen yksittäinen virhe useimmiten käynnistää tapahtumaketjun, jolla on pahimmillaan vakavia seurauksia. Kehittyneestä teknologiasta huolimatta teknisten ympäristöjen suurin uhka on ihminen itse. (Voss 2001, 1)

3.2 Henkilöstötietoturvan uhkatekijät

Yritysten ulkopuolisten uhkatekijöiden, kuten rikollisten lisäksi tietoturvaa uhkaavat myös organisaatioiden ja yritysten omien työntekijöiden toiminta. Järjestelmiin voidaan esimerkiksi murtautua haittaohjelmin tai tietomurroin, mutta myös henkilöstöä voidaan hyödyntää tietojen saamiseksi. Ihmisten toimintaan saatetaan pyrkiä vaikuttamaan siten, että se on tietoja haluavalle taholle suotuisaa. Aina tätä vaikuttamista ei kuitenkaan edes tarvita. Ihminen saattaa omalla huolimattomalla toiminnallaan antaa tietoja vääriin käsiin ilman, että häneen on mitenkään vaikutettu ulkopuolisen tahon toimesta.

3.2.1 Social Engineering

Social engineering eli käyttäjien manipulointi tai sosiaalinen manipulointi on ihmisten huijaamista siten, että he luovuttavat luottamuksellista tietoa sitä kalastelevalle taholle. Tavoitteena on saada käyttäjältä esimerkiksi salasanoja tai lupa käyttää tämän tietokonetta esimerkiksi etäyhteyden avulla. Tähän vaaditaan sosiaalisia taitoja ja käyttäjä on pystyttävä vakuuttamaan, jotta tältä saataisiin kerättyä haluttuja tietoja. Ihmiseen vaikuttamista ja tämän taipumusten hyväksikäyttöä pidetään kuitenkin helpompina vaihtoehtoina kuin sitä, että murtauduttaisiin esimerkiksi tietokoneen sovelluksiin. Konkreettinen esimerkki tästä on salasanan hankkiminen käyttäjää huijaamalla sen sijaan, että sitä lähdettäisiin murtamaan sitä. (Criddle 2016.)

Social engineering voidaan jaotella erilaisiin menetelmiin, joilla pyritään vaikuttamaan käyttäjään ja saamaan tältä tietoja. Näitä menetelmiä on valtavasti, mutta esimerkiksi

phishing, baiting sekä tailgating ovat yleisiä ja hyviä esimerkkejä social engineeringin toimintamenetelmistä. (Bisson 2015; Criddle 2016.)

Phishing

Phishing (tietojenkalastelu) on rikollisen käyttämä keino saada tietoja käyttäjältä. Phishing tarkoittaa tietojen kalastelua siten, että käyttäjä pyritään vakuuttamaan lähettämällä sähköposti- tai tekstiviestejä luotettavilta vaikuttavilla nimikkeillä. Tyypillinen esimerkki tästä on sähköpostiviesti, jossa käyttäjälle ilmoitetaan tämän voittaneen arvonnassa esimerkiksi suuren summan rahaa. (Tietosuojavaltuutetun toimisto 2010; Criddle 2016.)

Baiting

Baiting (syötillä huijaaminen) on phishingin kaltainen tiedonkalastelumenetelmä, jossa käytetään syöttinä jotakin hyödykettä tai tavaraa. Jotta käyttäjä saisi ilmoitetun hyödykkeen tai esineen omakseen, tulee tämän luovuttaa usein tietoja vastapalvelukseksi. Nämä tiedot voivat olla esimerkiksi kirjautumistietoja sisältäen käyttäjätunnuksen ja salasanan. Erilaiset helposti saatavissa olevat hyödykkeet kiinnostavat ihmisiä ja he tarttuvat syöttiin. Hyödykkeitä, kuten ilmaisia muistitikkuja voidaan myös täyttää haittaohjelmilla ja antaa käyttäjille suoraan, tai esimerkiksi levittää niitä työpaikalla. Lattialla oleva muistitikku herättää kiinnostusta, ja sen sisällöstä kiinnostunut käyttäjä saattaa kytkeä sen yrityksen tietokoneeseen. (Bisson 2015.)

Tailgating

Tailgating (tiloihin kulku pääsyoikeuden omaavaa henkilöä seuraamalla) on hyvä esimerkki siitä, ettei kaikki social engineering tapahdu sähköisessä muodossa. Tailgatingissä pääsyoikeudeton rikollinen pyrkii pääsemään suojattuun tilaan tai yrityksen tiloihin seuraamalla oikeudenhaltijoita, kuten yrityksen työntekijöitä. Rikollinen voi esimerkiksi odottaa yrityksen ulko-oven edustalla sitä, että työntekijä kulkisi yrityksen lukitusta ovesta sisään. Kun ovi on auki ja työntekijä siirtyy huolettomasti yrityksen tiloihin, avautuu rikolliselle tilaisuus päästä sisälle. Kohteliaisuus on tailgatingissä avainasemassa, sillä rikollinen saattaa tarjoutua pitämään avattua ovea auki tai yrittää

keskustella tuttavallisesti yrityksen työntekijän kanssa. Huomion siirtäminen turvallisuudesta muihin asioihin edesauttaa rikollisen pääsyä haluttuun kohteeseen. (Bisson 2015.)

Eri ihmiseen vaikuttamisen menetelmiä voidaan myös yhdistää, ja yhdessä tietojenkalasteluyrityksessä voidaan käyttää erilaisia keinoja. Erilaisia variaatioissa vain mielikuvitus on rajana. Näin niiden hahmottaminen voi olla käyttäjille haastavaa.

3.2.2 Itse käyttäjä tietoturvauhkana

Yrityksen oma työntekijäkin saattaa olla tietoturvauhka yritykselle. Tähän ei vaadita välttämättä lainkaan social engineeringin kaltaisia menetelmiä, vaan huolimaton toiminta oman työn ohessa voi johtaa tietojen päätymiseen ulkopuolisten käsiin. Työtahti saattaa olla kiivas ja kiireessä tietoturva-asiat jäävät valitettavan usein toissijaisiksi. Osaamattomuus tietoturva-asioissa, väärä asenne ja mahdolliset erimielisyydet työnantajan kanssa saattavat myös johtaa arkaluontoisten tietojen päätymisen julkisuuteen tai kilpailijoiden käsiin.

Omien työtehtävien vaivaton ja nopea suorittaminen on se, mitä työntekijä eniten arvostaa. Kiireelliset aikataulut ajavat käyttäjän asettamaan työtehtävän valmistumisen tietoturvan edelle. Esimerkiksi tietokoneella työskennellessä työntekijän eteen saattaa avautua ikkunoita, joissa pyydetään hyväksymään jotain tai siirtymään prosessissa eteenpäin. Kiireessä käyttäjä klikkaa eteenpäin ja seurauksena saattaa olla tietojen menetyksiä tai muita vakavia seuraamuksia. Etenkin kiireessä ilmenevä huolimattomuus voi ilmetä myös sähköpostiviestien päätymisessä väärille henkilöille tai vääriä tiedostoja päätyy vääriin paikkoihin. Kiireen ja huolimattomuuden seurauksena virheet voivat olla ikuisia ja levitä jopa maailmanlaajuisesti. (Järvinen 2012, 25.)

Henkilöstön osaamattomuus tietoturva-asioissa on myös kriittinen tietoturva-uhka yritykselle. Työntekijät ovat itse vastuussa siitä, että he suorittavat työtehtävänsä tietoturvallisesti. Valtaosa työntekijöistä haluaakin toimia oikein ja tehdä työnsä tietoturvallisesti. Tämän tukemiseksi ja tietoturvallisen toiminnan varmistamiseksi tarvitaan kuitenkin asianmukaista ohjeistamista ja kouluttamista. (Laaksonen ym. 2006, 143.)

Kaikki työntekijät eivät kuitenkaan halua välttämättä toimia annettujen ohjeiden mukaisesti. Vääränlainen asenne ja piittaamattomuus tietoturva-asioissa ovat nekin

ongelmallista yrityksille. Tietoturva voidaan nähdä välttämättömänä pahana, joka hidastaa omaa työntekoa. Työtehtävät hoidetaan mahdollisimman nopeasti, piittaamatta käyttöohjeista ja tietoturva-asiat jätetään tietohallinnon murheeksi. (Järvinen 2012, 24–25.)

Työntekijä saa työsuhteensa aikana tietoja yrityksestä, tuotteista, toimintatavoista ja muista ainakin osittain salassa pidettävistä asioista. Työsuhteen päättyessä näitä tietoja lähtee työntekijän mukana ja esimerkiksi yrityssalaisuudet voivat päätyä kilpailijalle tai muuten julkiseksi. Vakavan tietovuodon toteutuvuuteen vaikuttaa merkittävästi työsuhteen päättymisen syy. Mikäli työntekijä on lähtenyt vääränlaisen toiminnan tai riidan seurauksena, on riski suurempi kuin esimerkiksi eläkkeelle siirtymisen yhteydessä. (Laaksonen ym. 2006, 144.)

3.2.3 Työntekijä ja sosiaalisen median vaarat

Sosiaaliset mediat, kuten Facebook ja Twitter ovat oikein käytettyinä oiva tapa edistää yrityksen liiketoimintaa tai hankkia kilpailuetua kilpailijoihin nähden. Mikäli sosiaalista mediaa käytetään työntekijöiden toimesta väärin, yrityksen maine ja liiketoiminta saattavat kärsiä merkittävästi. Työtekijöiden toiminnan kautta rikollisille avautuu myös mahdollisuuksia sosiaalisen manipuloinnin keinojen hyödyntämiseen. Sosiaalisessa mediassakin ihminen on kuitenkin suurin tietoturvauhka. Työntekijöiden hallitsematon verkostoituminen esimiestensä kanssa, negatiiviset ilmaukset yrityksestä ja jopa suorat tietovuodot yrityksen liikesalaisuuksista tai ongelmista ovat esimerkkejä tietoturvan kannalta huonosta toiminnasta. (Andreasson & Koivisto 2013, 163; Touhill, G. & Touhill, J. 2014, 48–49.)

Hallitsemattomassa verkostoitumisessa ongelmana on se, että rikolliset tahot pystyvät muodostamaan suhteellisen helposti organisaatiokaavioita ja hahmottamaan henkilöiden toimenkuvia yrityksessä. Negatiivisten mielipiteiden julkaisu on sosiaalisessa mediassa helppoa matalan julkaisukynnyksen takia. Tällainen toiminta on ongelmallista etenkin yrityksen maineen kannalta ja esimerkiksi tuotanto-ongelmista viestiminen sosiaalisessa mediassa vaikuttaa helposti yrityksen taloudelliseen menestykseen. Suorat tietovuodot esimerkiksi uusista tuotteista ovat myös mahdollisia ja etenkin kilpailijat ovat kiinnostuneita tällaisista tiedoista. (Andreasson & Koivisto 2013, 163; Touhill, G. & Touhill, J. 2014, 49.)

Sosiaaliseen mediaan liittyy paljon tietoturvaongelmia, mutta oikein käytettynä ja käytön ollessa valvottua siitä voi olla runsaasti hyötyä. Yrityksille se voidaan nähdä näkyvyyttä ja liiketoiminnan kasvua edesauttavana sekä viestintää nopeuttavana työkaluna. (Touhill, G. & Touhill, J. 2014, 49.)

Yrityksen henkilöstö on avainasemassa onnistuneen tietoturvakokonaisuuden toteutumisessa. Tietoturvaa uhataan henkilöstön toimesta tahattomasti ja tahallaan. Tietoihin pyritään pääsemään käsiksi myös heidän varomattomuuttaan ja osaamattomuuttaan hyväksi käyttäen. Työntekijöiden tietoturvallista toimintaa ei tule pitää itsestäänselvyytenä, ja sitä tulee seurata sekä edistää muun toiminnan ohessa.

4 TIETOTURVAOSAAMISEN KARTOITTAMINEN JA KEHITTÄMINEN

Henkilöstöön kohdistuvat ja heidän toiminnastaan aiheutuvat tietoturvauhat tulee tiedostaa, jotta toimintaa voidaan lähteä kehittämään oikeaan suuntaan. Jatkuvan tietoturvauhan vuoksi henkilöstön tietoturvatietoisuutta tulee lisätä ja pyrkiä aktiivisesti havaitsemaan mahdolliset tietoturvapuutteet henkilöstön toiminnassa. Oikeanlaisella toiminnalla mahdollisten erheiden määrää saadaan vähennettyä ja turvallisuustoimintoja pystytään hyödyntämään tehokkaasti. (Lacey 2009, 211.)

Tietoturvatason yleiseen arviointiin on erilaisia menetelmiä, joita voidaan hyödyntää eri tavoin eri organisaatioissa. Menetelmien soveltuvuus organisaatioille riippuu esimerkiksi toimialasta, organisaatiokulttuurista ja käytössä olevista järjestelmistä. Yrityskäyttöön soveltuvia menetelmiä ovat esimerkiksi riskianalyysit, tietoturvahaavoittuvuuksien etsintä, työntekijöiden toiminnan tietoturvallisuuden arviointi, tietoturvatoiminnan vertaaminen tietoturvastandardeihin sekä erilaiset tarkastuslistat. (Laaksonen ym. 2006, 272–273.) Tietoturva-arviointeihin kuuluu henkilöstön lisäksi merkittävänä osana myös sovellusten, tietojärjestelmien ja tietoteknisten laitteiden tarkastaminen. Tässä opinnäytteessä perehdytään kuitenkin vain henkilöstön tietoturvallisuuden arviointi- ja kehitysmenetelmiin.

Arvioinnin jälkeen havaitut puutokset käydään läpi ja niiden pohjalta voidaan laatia henkilöstön tietoturvan kehittämiseen tähtääviä toimenpiteitä. Työntekijöiden tietoturvaosaamista voidaan tehokkaasti lisätä esimerkiksi koulutuksilla ja motivoimalla heitä toimimaan tietoturvallisemmin työpaikalla ja oman työn ohessa.

4.1 Toimintamallit ja tietoturvastandardit

Tietoturva-arviointeja ja muita tietoturvan kehitystoimenpiteitä voidaan toteuttaa erilaisten toimintamallien ja standardien ohjeistuksen mukaisesti. Toimintamallit ovat yleisesti tunnettuja malleja valmiiksi kehitetyistä ratkaisuista. Esimerkki tunnetusta toimintamallista on COBIT (Control Objectives for Information and Related Technologies). COBIT muodostuu monesta hyväksi havaitusta IT-hallinnon käytännöstä. COBIT on mallina monimutkainen ja raskas, koska se vaatii organisaatiolta runsaasti eri

politiikkoja, toimenpiteitä ja dokumentaatiota. Standardit ovat puolestaan organisaatioiden suosituksia asioiden oikeanlaiseen hoitamiseen. Tietoturvan kehittämisen kannalta merkittävä standardikokonaisuus on ISO:n (International Organization for Standardization) ja IEC:n (International Electrotechnical Commission) 27000-standardisarja. Kattavan sarjan standardit antavat hyviä ohjeita tietoturvan hallintaan, arviointiin ja kehittämiseen. (Flat Iron Technologies 2014; IT Governance 2016.)

Mallien ja standardien käyttö arvioinneissa ja mittauksissa ei ole välttämätöntä, ellei kyseessä ole niiden vaatimuksiin suoraan perustuvat tarkastukset tai mittaukset. Tässä opinnäytetyössä käytettävät arviointi- ja kehitysmenetelmät eivät perustu suoraan tietoturvastandardeihin tai -malleihin, eikä taustalla ole vaatimuksia niiden hyödyntämiseen. Tarkoituksena on ensisijaisesti verrata olemassa olevia kartoitus- ja kehitysmenetelmiä sekä käydä läpi aikaisemmin järjestettyjä mittauksia ja koulutuksia.

4.2 Henkilöstön tietoturvatason kartoitusmenetelmät

Henkilöstön tietoturvaa mitattaessa keskitytään ihmisen käyttäytymiseen ja toimintaan. Työntekijän toiminnan arviointi on haastavaa, koska se saattaa vaikuttaa tämän mielialaan ja tehokkuuteen työpaikalla. Työntekijöitä tulee arvioida oikeudenmukaisesti, mutta silti asioista tulisi puhua suoraan ja niin kuin ne ovat. Suorasanainen arviointi ei kuitenkaan saisi olla syyllistävää ja painottaa vain epäkohtia. Pienissä yrityksissä mittaukseen tulisi saada mukaan kaikki yrityksen työntekijät. Suuremmissa yrityksissä kohteeksi valitaan yleisen ohjeistuksen mukaan pienempi ryhmä, jolla saadaan kokonaistilannetta hahmoteltua. (Laaksonen ym. 2006, 278–279.) Suurissakin yrityksissä voidaan ottaa mukaan koko henkilöstö, mutta suuremmat tietoturvakampanjat vaativat usein runsaasti työtä ja resursseja.

Tyypillisiä keinoja henkilöstön tietoturvallisuuden mittaamiseen ovat erilaiset tarkistuslistat ja kyselyt. Tietoturvasta vastaavat voivat seurata työntekijöiden toimintaa valmiiksi laadituilla listoilla, joissa tarkastettavat kohteet pysyvät samoina. Listat voivat sisältää esimerkiksi havaittujen lukitsematta jääneiden tietokoneiden määrän toimistolla tai työhön liittyvän salaisen dokumentaation määrän työpisteillä. Henkilöstölle voidaan myös laatia tietoturvakyselyitä, joilla mitataan yleisesti tietoturvatietämyksen tasoa tai esimerkiksi yrityksessä ajankohtaisina olevia tietoturva-asioita. (Laaksonen ym. 2006, 278–279.)

4.2.1 Tarkistuslistat

Henkilöstön toiminnan seuraaminen tarkistuslistojen avulla on etenkin johdolle ja tietoturvapäälliköille hyvä menetelmä mitata työntekijöiden tietoturvatietoisuuden ja tietoturvallisen käyttäytymisen tasoa. Tarkistuslistojen avulla seurantaa on helppo toteuttaa säännöllisin väliajoin, eikä se vaadi ulkopuolisia henkilöitä tai runsaasti resursseja. (Laaksonen ym. 2006, 279.)

Yksinkertaisimmillaan listat koostuvat seurattavasta asiasta sekä kielteisestä tai myönteisestä arviosta. Arvioitavaa toimintaa voidaan myös esimerkiksi pisteyttää ja näin laatia kattavampaa arviointia tarkistuslistojen perusteella. Taulukossa 1 on esitetty yksinkertainen esimerkki tarkistuslistasta, jossa on arvioitavalle kohteelle ja arvioinnin tuloksille omat sarakkeensa. Tämän tyyppiset tarkastuslistat sopivat erityisesti toimistotyötä tekevien työntekijöiden arviointiin.

Taulukko 1. Esimerkki yksinkertaisesta tarkistuslistasta.

Arvioitava kohde	**Kyllä**	**Ei**
Työpisteellä paperidokumentit ovat levällään.		
Tietokone on jätetty lukitsematta käyttäjän poistuttua.		
Työntekijän työpöydällä on muistitikkuja näkyvissä.		
Salasanat on kirjoitettu näkyvissä olevalle muistilapulle.		
Kulkukortti tai muu yrityksen tunnistautumisväline on jätetty työpisteelle näkyviin.		
Työntekijä vastasi sähköpostitse lähettämääni tietojenkalasteluviestiin.		

Tarkkojen ja kattavien tulosten saamiseksi tarkistuslistoissa on hyvä olla useampi arvioitava kohde. Yksinkertaisellakin tarkistuslistalla voidaan kuitenkin mitata tehokkaasti tietoturvatietoisuutta ja -osaamista. Esiintyvien puutteiden pohjalta voidaan laatia tarvittavat toimenpiteet tietoturvatason nostamiseksi.

4.2.2 Kyselyt

Tietoturvakysely on perinteinen tapa mitata työntekijöiden tietämystä tietoturvasta, tietoturvakäytännöistä ja -standardeista. Mikäli yrityksellä on ollut tietoturvan kehittämiseen tähtäävää toimintaa, kyselyillä voidaan myös mitata tietoturvatoiminnan tehokkuutta. Kyselyillä voidaan myös selvittää ihmisten ajatuksia tietoturvasta ja sitä, kuinka vakavasti he suhtautuvat tietoturvaan ja sen haasteisiin. Näihin aihepiireihin liittyviä kyselyitä on helppo laatia ja niiden avulla saadaan paljon tietoa turvallisuuden kehittämiseen tähtäävien toimenpiteiden hahmottamiseksi. Vaikka kyselyiden laatiminen on selkeää, niihin liittyy tiettyjä haasteita. Kysymysten heikko rajaaminen tai vastausten väärin tulkitseminen tekevät pahimmassa tapauksessa koko arvioinnista täysin pätemättömän. (Lacey 2009, 213–214; Bond 2012, 1.)

Kysymyksistä voidaan tehdä joko johdattelevia tai johdattelemattomia. On suositeltavaa tehdä johdattelemattomia kysymyksiä, mikäli ei haluta vaikuttaa mittaustuloksiin. Lisäksi kyselyihin voidaan valita joko avoimia kysymyksiä tai suljettuja kysymyksiä. Avoimet kysymykset soveltuvat hyvin mittauksiin, joista halutaan kerätä enemmän tutkimusaineistoa. Ne mahdollistavat sen, että tietoturva-arviointiin osallistuvat kohdehenkilöt voivat avoimesti pohtia kysymyksiä. Näin vastauksista saadaan avoimia ja monipuolisempia. Avointen kysymysten analysointi on kuitenkin raskasta ja se vie etenkin suurten henkilömäärien yhteydessä paljon aikaa. Suljetut kysymykset ovat varteenotettava vaihtoehto silloin, kun vastausten analysointiin ja prosessointiin ei haluta käyttää niin paljoa aikaa ja resursseja. Nämä kysymykset ovat tyypillisesti monivalintakysymyksiä, joissa annetuista vastausvaihdetuista valitaan yksi. (Lacey 2009, 214.)

Kyselyiden avulla kerätty aineisto voidaan käsitellä käsin tai koneellisesti. Käsin tehtävä käsittely voi olla äärimmäisen työlästä, jos aineistoa on runsaasti. Koneellinen prosessointi on suositeltavaa, mutta se ei ole käytetyistä kyselymenetelmistä riippuen aina mahdollista. Aineiston käsittelytavasta riippumatta kerätty materiaali on hyvä pitää yhdessä paikassa sekä selkeästi yhdenmukaisesti esitettynä. (Lacey 2009, 215.)

Suunnittelu, testaaminen ja tulevaisuuden huomioiminen ovat hyvän kyselyn perusta. Kyselyitä ei tule pitää nopeana ratkaisuna organisaation tietoturvaongelmiin, vaan ne tulee nähdä osana pitkäaikaista tietoturvaohjelmaa tai -kampanjaa. (Lacey 2009, 215.)

Henkilöstön tietämys tietoturva-asioista on liiketoiminnan kannalta merkittävää ja sen mittaamiseksi on eri vaihtoehtoja ja menetelmiä. Valitusta menetelmästä riippumatta mittaaminen on suositeltavaa, jotta toiminnan haavoittuvat kohdat voidaan tunnistaa. Vasta toiminnan nykytason selvittämisen jälkeen voidaan laatia oikein kohdistetut toimet tietoturvatason parantamiseksi yrityksessä tai organisaatiossa.

4.3 Kehitysmenetelmät

Henkilöstön tietoturvatietoisuuden ja -osaamisen kehittäminen perustuu laaditun etenkin tietoturvapolitiikan ja muun tietoturvaohjeistuksen kertaamiseen sekä havaittujen puutteiden korjaamiseen. Työntekijöiden toimintaa voidaan viedä tietoturvallisempaan suuntaan sääntöjen ja rajoituksien avulla. Valtavalla määrällä erilaisia säännöksiä ja rajoitteita voi olla kuitenkin negatiivinen vaikutus ihmisten käyttäytymiseen ja motivaatioon. Tämän takia kehityksen kannalta tärkeää on luoda tehokasta turvallisuuskulttuuria, motivoida henkilöstöä oppimaan ja järjestää työntekijöille oikeantyyppistä koulutusta. (Laaksonen ym. 2006, 279; Brook & Sharma, 2016.)

4.3.1 Tietoturvaohjeistus

Yksi tärkeimmistä tietoturvan kehittämisen osista on organisaatiossa laadittu tietoturvaohjeistus ja -dokumentaatio. Tietoturvaan liittyviä ohjeita laaditaan organisaation eri tarkoituksiin ja ne vastaavat tiettyjä vaatimuksia. Nämä vaatimukset löytyvät yritysten tietoturvapolitiikasta, jossa ne on esitetty selkeästi ja hyvin yleisellä tasolla. (Laaksonen ym. 2006, 145.)

Tietoturvaohjeiden laatiminen on keskeinen osa yritysten tietoturvaohjelmia ja -kampanjoita, joissa kerrotaan tietoturvan parantamistoimet ja niiden toteutustavat (Laaksonen ym. 2006, 250). Laadittavien ohjeiden tulee olla selkeitä ja niiden tulee olla linjassa aikaisemmin laadittujen ohjeiden kanssa. Epäselvät ohjeet aiheuttavat hämmennystä ja tekevät ohjeista helposti merkityksettömiä. (Laaksonen ym. 2006, 145–146.) Ohjeistusta laadittaessa johdolla ja tietoturvahenkilöstöllä tulee olla tarkkaan harkitut syyt ohjeiden muodostamiseksi. Yksi hyvä syy on lista tietoturvapuutteiden kartoittamisen seurauksena ilmenneistä havainnoista. (Laaksonen ym. 2006, 250.)

Tietoturvaohjeet antavat hyvän pohjan tietoturvakehitykselle. Tietoturvaohjeet eivät kuitenkaan yksinään riitä, vaan tueksi tarvitaan myös henkilöstön kouluttamista.

4.3.2 Tietoturvakoulutus

Tietoturvatietoisuutta ja kattavaa tietoturvaosaamista voidaan lisätä kouluttamalla henkilöstöä. Koulutustoiminnan suunnittelussa lähdetään liikkeelle olemassa olevasta tietoturvapolitiikasta, toimintaohjeista, prosessikuvauksista sekä henkilöstön toiminnan tietoturvapuutteista. (Laaksonen ym. 2006, 254.) Tietoturvakoulutusta suunniteltaessa on tärkeää ottaa huomioon myös seuraavat asiat:

- Tietotekniikan käyttäjien kokonaislukumäärä yrityksessä
- Käyttäjien nykyiset IT- ja tietoturvataidot
- Henkilöstön käsittelemän tiedon kriittisyys ja salaisuus
- Yrityksen tietoturvakäytännöt
- Yritystä koskevat juridiset tai teolliset toimeksiantosopimukset
- Yrityksen tietoturvahenkilöstön osaaminen ja työkuorma
- Käytettävissä oleva rahamäärä.

(Shinder 2013a.)

Suunnitteluvaiheessa valitaan myös koulutuksen toteutustapa. Henkilöstöä voidaan kouluttaa monella eri tavalla ja eri koulutustyyppejä on mahdollista yhdistää mielenkiintoiseksi ja tehokkaaksi kokonaisuudeksi. Tyypillisiä koulutusmenetelmiä ovat perinteiset luokkatiloissa pidettävät koulutukset ja PowerPoint-esitykset. Kaikille perinteinen koulutus ei ole paras vaihtoehto ja siksi on tarjottava erilaisia tapoja asian ymmärtämiseksi. Vaihtoehtoisia menetelmiä ovat erilaiset tietoiskut, paneelikeskustelut ja työpajat. Näissä menetelmissä työntekijöitä pyritään aktivoimaan ja saamaan aikaan keskustelua aiheesta. Lisäksi henkilökuntaa voidaan kouluttaa tietokoneilla tehtävin verkkokoulutuksin ja käytännön harjoittein, joissa IT-laitteita hyödynnetään koulutuksen tehostamiseksi. (Laaksonen ym. 2006, 257–260; Shinder 2013b.)

Tietoturvakoulutus voidaan järjestää yrityksen oman henkilökunnan toimesta, mutta on myös mahdollista ottaa ulkopuolinen henkilö järjestämään koulutuksia. Yritysten sisällä koulutuksista vastaavat IT-osastot tietoturvaorganisaatioineen sekä joskus osittain myös henkilöstöosasto. (Laaksonen ym. 2006, 259: Shinder 2013a.)

Oman yrityksen sisältä tuleva kouluttaja nähdään tuttuna henkilönä ja näin koulutettava yleisö on vastaanottavampi koulutuksen suhteen. Ulkopuoliseen kouluttajaan kuitenkin suhtaudutaan usein kunnioittavammin ja tämä nähdään enemmän tietyn koulutettavan aiheen ammattilaisena. Lisäksi ulkopuolisella on puolueeton näkökulma ja näin tuloksista ei tule liian positiivissävytteisiä. Valintaa tehdessä tulee huomioida se, että sisäiset kouluttajat sekä heidän toimintatapansa ja osaamisensa tunnetaan hyvin. Ulkopuolisen tahon järjestämien koulutusten tasosta ja koulutusmenetelmien toimivuudesta ei voida olla varmoja. Siksi ulkopuolisia kouluttajia tulee vertailla ja ottaa selvää heidän tarjoamista koulutuksista. (Shinder 2013a.)

Raha ja aika ovat merkittävässä osassa tietoturvakoulutuksen järjestäjän valinnassa. Omaa henkilökuntaa käytettäessä voidaan ajatella säästettävän rahaa. Kattavat koulutukset vaativat usein paljon työtä ja mikäli ylityötunteja kertyy merkittävästi, tulee huomioida muiden töiden mahdollinen kasaantuminen ja ylityökustannukset. Yksi hyvä toimintatapa yleisen tason tietoturvakoulutuksiin on ottaa esimiehet alaistensa kouluttajiksi. Esimerkiksi yleisen tason tietoturvaohjeistuksista ilmoittamiseen ei välttämättä vaadita koko tietoturvaorganisaation panosta, vaan esimies voi tiedottaa alaisiaan. (Laaksonen ym. 2006, 258: Shinder 2013a.)

Henkilöstön kouluttaminen on lähtökohtaisesti monesta syystä haastavaa. Aikuisten kouluttaminen työpaikan luokkatiloissa saattaa tuntua heistä vastenmieliseltä. Lisäksi he eivät missään nimessä halua vaikuttaa tietämättömiltä, eivätkä sen vuoksi kysy mielellään kysymyksiä tai selvennyksiä heille koulutuksessa epäselviksi jääneisiin asioihin. (Shinder 2013b.)

Haasteita asettavat henkilöstön ajatusmaailman lisäksi myös tilajärjestelyt, aikataulutus sekä koulutettavien ryhmien koko. Etenkin suurissa organisaatioissa samoja yksittäisiä tiloja voi olla haastavaa saada varattua pitkäaikaisiin koulutusohjelmiin. Kooltaan, esitysmahdollisuuksiltaan ja sijainniltaan parhaan koulutustilan valinnassa eteen voi tulla yllätyksellisiä vierailuja tai muita tärkeitä tapahtumia, eikä haluttua tilaa saadakaan käyttöön. Tilajärjestelyjen lisäksi aikataulutus on merkittävä haaste, ja koulutuksen kestoa sekä ajankohtaa työpäivän sisällä tulee miettiä. Tilaisuuden tulisi olla kestoltaan oikea ja sopivaan aikaan työpäivästä, jotta mahdollisimman moni saapuisi paikalle. Koulutettavien ryhmien koon määrittäminen voi olla myös haastavaa. Liian pienessä ryhmässä keskustelua on vaikea saada syntymään. Isossa ryhmässä kouluttajan on puolestaan vaikea keskittyä yksilöihin ja olla mukana keskustelussa. (Shinder 2013b.)

Tietoturvakoulutukset ovat hyvä tapa kehittää henkilöstön tietoturvaa organisaatiossa. Kouluttamisen eri menetelmät, kouluttajan valinta ja koulutusten järjestämiseen liittyvät haasteet tulee kuitenkin tarkasti huomioida hyvän ja miellyttävän koulutuksen varmistamiseksi.

4.3.3 Motivointi

Tietoturvaohjeita laatimalla ja erilaisia koulutuksia järjestämällä henkilöstön tietoturvatietoisuus ja tietoturvan taso saadaan lähtökohtaisesti paremmalle tasolle. Kehittämistoiminta on kuitenkin hyödytöntä, mikäli henkilökunta ei ole motivoitunut kehitykseen. (Laaksonen ym. 2006, 252–253.)

Työntekijöitä voidaan motivoida ja tietoturvallisuutta parantaa myönteisten kannustimien avulla. Positiiviset kannustimet ja työntekijöiden palkitseminen kohottavat ilmapiiriä. Kohonnut ilmapiiri luo puolestaan perustan henkilöstön yhteistyölle ja tietoturvallisuuden kehittämiselle. (Laaksonen ym. 2006, 252–253.)

4.4 Esimerkkejä tietoturvakartoittamisesta ja -kehittämisestä

Henkilöstön toiminnan tietoturvallisuuden tasoa ja tietoturvatietoisuutta on kartoitettu ja lisätty yrityksissä ja muissa organisaatioissa eri menetelmillä. Aikaisempia esimerkkikyselyitä ja -koulutuksia tarkastelemalla saadaan selkeämpi käsitys niiden sisällöstä, tarkoituksista ja mahdollisista tuloksista. Aikaisempien koulutusten tai kartoitusten tutkimisen jälkeen on myös helpompi lähteä suunnittelemaan omia henkilöstöä koskevia tietoturvamittauksia tai -koulutuksia. Mikäli esimerkiksi koulutustilaisuus on suunniteltu vain omien tietojen pohjalta, sillä ei saada välttämättä haluttua muutosta aikaan. Järjestettävään koulutustilaisuuteen voidaan ottaa muista tutkimuksista tai mittauksista menetelmiä, jotka koetaan hyviksi omia tavoitteita ajatellen. Pois voidaan jättää puolestaan ne menetelmät tai työvaiheet, joita ei nähdä tarpeelliseksi.

4.4.1 Verkkokysely osana Winnipegin tietoturvakartoitusta

Winnipegin kaupungin vuonna 2008 teettämässä tietoturvatietoisuuskartoituksessa ”The Assessment of Information Security Awareness” on mukana elektroninen kysely henkilöstön tietoturvatietoisuuden kartoittamiseksi (City of Winnipeg’s Audit Department 2008, 7). Kysely lähetettiin puolelle Internet-yhteyden omaavista kaupungin työntekijöistä eli noin 4 600 työntekijälle. Verkkokyselyyn saatiin 860 hyväksyttyä vastausta kuuden päivän aikana, jonka jälkeen tulokset analysoitiin. (City of Winnipeg’s Audit Department 2008, 18.)

Kyselyn sisältö on hyvin yksinkertainen ja siinä on kaksikymmentäviisi monivalintakysymystä. Työntekijöiltä pyydetään vastauksia esimerkiksi vieraan USB-tikun löytämisen ja tuntemattoman liitetiedoston vastaanottamisen jälkeisiin toimenpiteisiin. (City of Winnipeg’s Audit Department 2008, 22–23.)

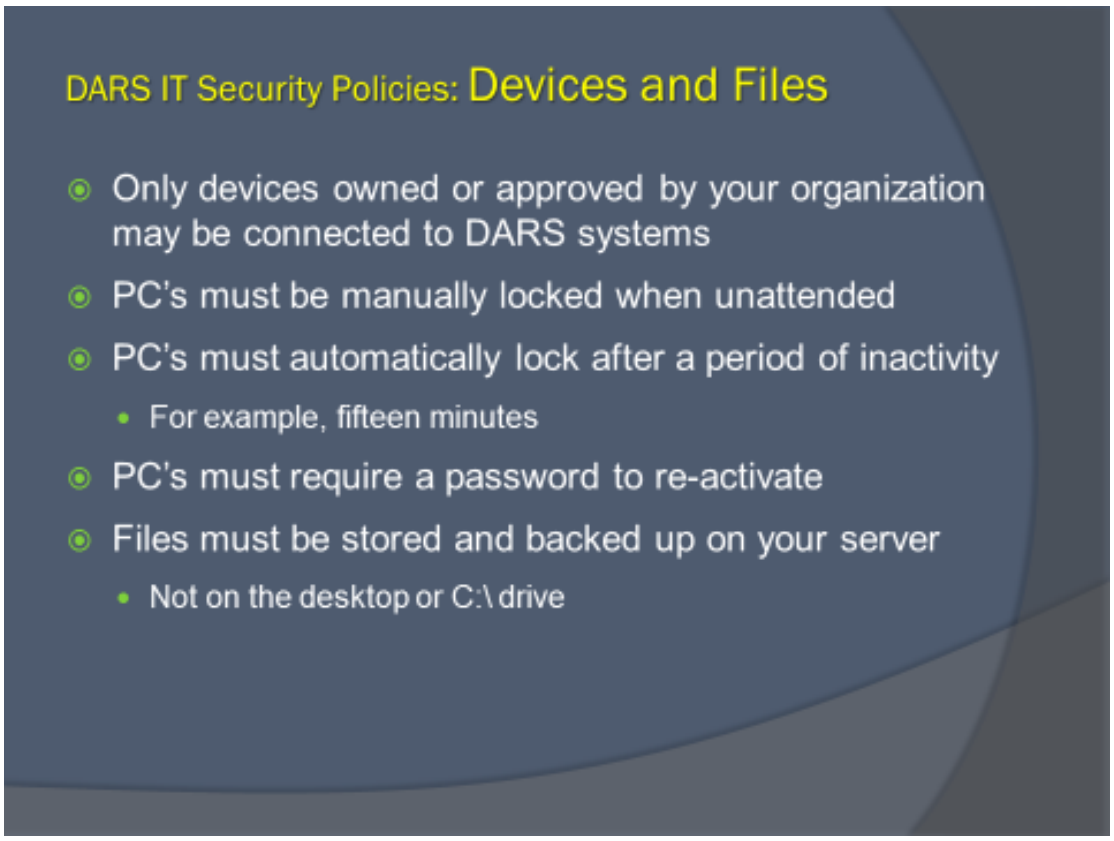
Kyselyn tuloksissa on positiivisia havaintoja ja parannusehdotuksia henkilöstön tietoturvatason kohottamiseksi. Positiivisissa havainnoissa korostetaan esimerkiksi työntekijöiden ymmärrystä yhteisestä tietoturvavastuusta. Parannuskohteita löytyi kyselyn avulla runsaasti ja niitä on eritelty kysymysjaottelun mukaan. (City of Winnipeg’s Audit Department 2008, 18–20.)

Winnipegin kaupungin työntekijöiden tietoturvakysely on hyvin toteutettu perinteinen tietoisuusmittaus. Verkkoa hyödyntämällä vastauksia on saatu tehokkaasti ja vähällä vaivalla. Monivalintatehtävät eivät mahdollista avoimia vastauksia, antavat selkeän kuvan työntekijöiden tietoturvaosaamisesta ja ymmärryksestä koskien kaupungin eri tietoturva-asioita.

4.4.2 VDARS:n tietoturvakoulutus loppukäyttäjille

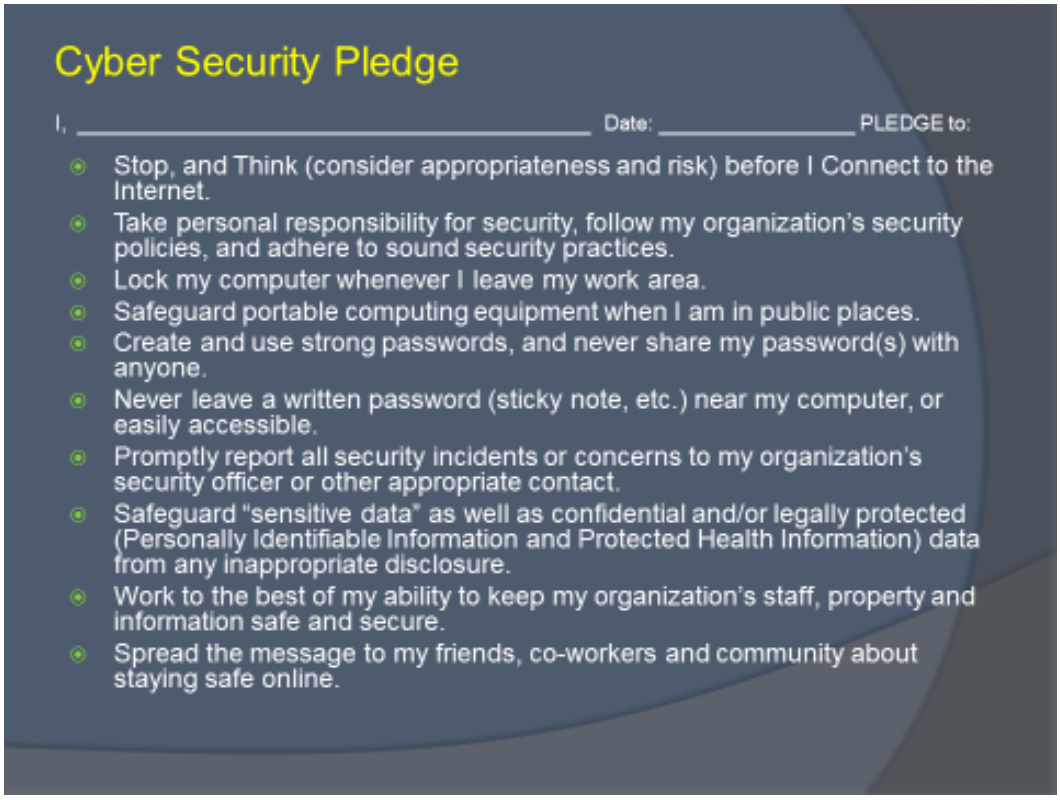
VDARS:n (Virginia Department for Aging and Rehabilitative Services) laati vuonna 2012 tietoturvakoulutuksen ”End User Cyber Security Training”. Koulutuksessa keskitytään niiden loppukäyttäjien – eli tietoteknisiä laitteita ja järjestelmiä käyttävien työntekijöiden – kouluttamiseen, joilla on pääsy organisaation arkaluontoisiin tai salaisiin järjestelmiin ja tietoihin. (Virginia Department for Aging and Rehabilitative Services 2012, 2).

Koulutus on tyypiltään sähköisesti jaettu PowerPoint-esitys, jossa käydään läpi tietoturvallisen toiminnan periaatteita ja käytäntöjä, joita jokaisen asiaa koskevan työntekijän tulisi noudattaa organisaatiossa. Kuvassa 1 esitetään VDARS:n laitteita ja tiedostoja koskevia tietoturvakäytäntöjä. Lisäksi koulutusmateriaali sisältää laajasti erilaisia kyseistä organisaatiota ja heidän työntekijöitään koskevia tietoturvauhkia. Jokaisen uhkatekijän esittelyn jälkeen koulutuksessa esitetään virheellinen toimintatapa sekä oikea toimintamalli. (Virginia Department for Aging and Rehabilitative Services 2012, 3–14.)



Kuva 1. VDARS:n laitteiden ja tiedostojen tietoturvakäytännöt (Virginia Department for Aging and Rehabilitative Services 2012, 4).

VDARS:n laatima PowerPoint-esitys on kattava ja todella tiivis koulutuspaketti, jonka lopussa on sitoutuvuusdia (Kuva 2). Osallistuneet työntekijät allekirjoittivat sen vakuuttaakseen ymmärtäneensä vastuunsa ja toimivansa tietoturvallisesti.



Kuva 2. VDARS:n tietoturvakoulutuksen sitoutuvuusdia (Virginia Department for Aging and Rehabilitative Services 2012, 16).

VDARS:n tietoturvakoulutus on hyvin yksinkertainen esimerkki perinteisestä koulutuksesta. PowerPoint-materiaalin sisältö on selkeä koulutettavalle ja hyvin ymmärrettävissä. Käytettäessä sähköistä koulutusmateriaalia ei kuitenkaan voida olla varmoja, että koulutettavat ovat perehtyneet aiheeseen kunnolla. Kokonaisuudessaan VDARS:n koulutus on kattava, mutta sen tehokkuus riippuu paljon koulutettavan asenteesta.

4.4.3 NIELIT:n tietoturvatyöpaja

National Institute of Electronics and Information Technology (NIELIT) järjesti vuonna 2015 kyberturvallisuuteen eli tietojärjestelmien kokonaisvaltaiseen suojaamiseen ja kybertietoisuuteen liittyvän tietoturvatyöpajan ”One Day Workshop on Cyber Security Awareness”. Yksipäiväiseen työpajaan osallistui yhteensä 86 henkilöä. Työpajan pääkohderyhmänä olivat Manipurin – joka on yksi Intian osavaltioista – hallinnon työntekijät. Työpajan tarkoituksena oli lisätä osallistujien tietoisuutta Internetin,

kyberturvallisuuden ja tietokonemaailman eettisten kysymysten alueilta. (National Institute of Electronics and Information Technology 2015, 1.)

NIELIT:n työpajassa tietoturvaa käsiteltiin eri puhujien toimesta ja mukana oli myös teknisiä osuuksia, joissa käytiin läpi eri näkökulmia aiheeseen liittyen (National Institute of Electronics and Information Technology 2015, 1–2). Kuvassa 3 on havainnollistettu työpajan ja sen teknisen osuuden toteutusta yleisön osalta. Osallistujat on koottu yhteen tilaan, jolloin kouluttaminen ja asioista keskusteleminen on helppoa.

Kuva 3. NIELIT:n tietoturvatyöpajan tilatoteutus osallistujien osalta (National Institute of Electronics and Information Technology 2015, 9).

Esiintyjät ja kouluttajat olivat tässä työpajassa suuressa roolissa, ja heille oli annettu hyvät tilat esiintymiseen (Kuva 4). Puhujan on helppo kouluttaa tai esittää materiaalia valkokankaan avulla.

Kuva 4. NIELIT:n tietoturvatyöpajan tilatoteutus puhujien osalta (National Institute of Electronics and Information Technology 2015, 8).

Winnipegin kaupungin tietoturvatietoisuuskartoituksen osana ollut verkkokysely, VDARS:n omalle henkilöstölleen luoma koulutuspaketti ja NIELIT:n järjestämä työpaja ovat yksittäisiä esimerkkejä siitä, miten tietoturvaa voidaan mitata ja kehittää. Jokaisessa esimerkkimenetelmässä on omat piirteensä, mutta tietoturvan kehittäminen on niiden yhteinen päätavoite.

Sähköinen monivalintakysely on helppo laatia ja lähettää suurellekin ihmisjoukolle. Vastauksista saadaan selkeät ja niitä on helppo analysoida. Winnipegin verkkokyselyssä jätetään kuitenkin avoimen vastauksen mahdollisuus pois. Näin käyttäjiltä ei saada kerättyä avointa palautetta, eikä heille anneta mahdollisuutta avata vastauksien tai käyttäytymisen taustoja.

Koulutus on oma lukunsa, ja VDARS:n tietoturvaesitys on toimiva ratkaisu perustason tietoturvakoulutusta ajatellen. Uusille käyttäjille kohdistettu tiivis koulutuspaketti antaa organisaation henkilöstölle hyvät valmiudet toimia tietoturvallisesti oikein. NIELIT:n tietoturvakoulutus työpajamuodossa antaa mahdollisuuden keskusteluun, koska osallistujat ovat kaikki yhdessä tilassa. Työpajamuotoinen kouluttaminen vaatii

enemmän valmisteluja ja aikaa kuin perinteisemmät koulutukset, mutta niissä voidaan yhdistää esimerkiksi kouluttaminen ja aineiston kerääminen.

Erilaisia variaatioita tietoturvakartoituksista ja koulutuksista käytetään eri organisaatioissa tietoturvan kehittämiseksi. Henkilöstön osaamisen tai tietoisuuden mittaamisessa tärkeää on muistaa mahdollisuudet erilaisten menetelmien käyttöön ja yhdistämiseen. Kaikkea ei tarvitse tehdä myöskään itse, vaan arvioinnit, mittaukset ja koulutukset voidaan teettää myös ulkopuolisilla. Vaihtoehtoja henkilöstön tietoturvaosaamisen ja organisaation tietoturvan kokonaistason nostamiseen on tarjolla niin paljon, että niitä kannattaa vertailla tarkasti ennen kuin lopullisia päätöksiä tehdään.

Menetelmästä ja koulutuksen pitäjästä riippumatta henkilöstön tietoturvaosaamisen mittaaminen ja jatkuva kouluttaminen on äärimmäisen tärkeää. Tietoturva-asiat huonosti hallitseva ihminen on väistämättä tietoturvan heikoin lenkki niin yrityksissä kuin muissakin organisaatioissa. Oikein ja hyvin laadittu ohjeistus sekä säännöllinen kouluttaminen luovat vahvan pohjan tietoturvalliselle toiminnalle sekä vahvalle ja jatkuvalle liiketoiminnalle.

5 KOHDEYRITYKSEN TIETOTURVATYÖPAJAT

5.1 Tausta

Tietoturvatyöpajojen taustatiedot perustuvat yrityksen henkilöstön kanssa käytyihin keskusteluihin. Kohdeyrityksen tietoturvan kehittämiseksi aikaisemmin käynnistetty maailmanlaajuinen tietoturvaprojekti pitää sisällään kattavasti tietoturvan eri osa-alueiden nykytasojen läpikäynnin ja kehittämisen. Tietoturvaprojektin yksi tärkeimmistä osa-alueista on henkilöstön tietoturvallisuus. Henkilöstön tietoturvallisuuden kehittämisen yritys on päättänyt toteuttaa niin Suomessa kuin muissakin maissa tietoturvatietoisuuskampanjan avulla (Kuvio 2).

Kuvio 2. Yrityksen tietoturvatietoisuuden kehittämiskampanja vaiheittain.

Kampanjan aikana yritys on julkistanut yksinkertaisia avainperiaatteita henkilöstön toimintaohjeiksi ja järjestänyt niiden pohjalta verkkokoulutusta. Seuraavana askeleena kampanjassa on pienryhmätyöskentely tietoturvatyöpajoissa. Työpajatyöskentelyn jälkeen pyritään seuraamaan tietoturvakehitystä ja edistämään tietoturvataitoja aktiivisesti myös jatkossa.

5.2 Tavoitteet

Työpajatyöskentelyn pääpainopisteenä on henkilöstön tietoturvatietoisuuden lisääminen. Yleisenä tavoitteena on, että työntekijät edistävät opittuja taitojaan entisestään, pohtivat tietoturva-asioita itsenäisesti ja ryhminä sekä hyödyntävät tietoturvataitoja entistä tehokkaammin omassa työskentelyssään.

Suomen henkilöstön osalta tietoturvatyöpajoja pyritään hyödyntämään tietoturvakehityksen kannalta mahdollisimman tehokkaasti ja kattavasti. Työpajat toimivat koulutustilaisuuksina, jossa työntekijöiden tietoturvatietoisuutta ja -osaamista pyritään lisäämään. Tämän lisäksi työpajoista kerätään tutkimusaineistoa, jota analysoimalla tavoitteena on selvittää yrityksen henkilöstön toimintaa koskevat tietoturvaheikkoudet. Jatkoa ajatellen heikkouksien perusteella pohditaan lisäksi henkilöstön tietoturvallisuuden parannusehdotuksista.

5.3 Osallistuvat osastot

Tietoturvatyöpajat kohdistetaan yrityksen lähes koko Suomen henkilöstölle eli yli 800 työntekijälle mukaan lukien toimihenkilöt ja tuotannon sekä sen tukitoimien työntekijät. Turun ja Espoon toimihenkilöistä mukaan kutsutaan lähes jokainen. Tuotannon henkilöstöstä kutsutaan vain kymmenesosa, koska tuotannon ja tuotannon tukitoimissa työskentelevien työntekijöiden kokonaismäärä on suuri, tuotannon on jatkuttava taukoamatta ja heidän tietoturvahaasteensa ovat keskenään hyvin samanlaisia.

Kaiken kaikkiaan työpajoihin kutsutaan 523 työntekijää, joista 441 on yrityksen toimipisteissä työskenteleviä toimihenkiöitä. Pienemmät osallistujaryhmät muodostuvat tuotannon työntekijöistä (28), vuokratyöntekijöistä (49) ja myyntihenkilöstöstä (5). Myyntityötä eri puolella Suomea tekeviä henkilöitä on enemmänkin, mutta tietoturvatyöpajoihin kutsutaan vain yksi myynnin osasto.

Turun tuotantolaitokselta työpajoihin osallistuu 54 eri osastoa (Liite 1). Espoon toimistosta osallistuu puolestaan 27 eri osastoa (Liite 2). Lisäksi Espoon toimistolta tietoturvatyöpajoihin osallistuvat myös suurimmat vuokratyöntekijäosastot (Liite 3). Vuokratyöntekijät ovat merkittävä kohderyhmä yrityksen varsinaisten työntekijöiden lisäksi. He käyttävät samoja IT-laitteita ja pääsevät käsiksi pääosin samoihin osastokohtaisiin tietoihin kuin yrityksen omat työntekijät. Turun ja Espoon henkilöstön lisäksi työpajoihin otetaan mukaan myös ympäri Suomea liikkuvia ja kotitoimistoillaan työskenteleviä myyntihenkilöitä. Myyntihenkilöiden kiireellisen aikataulun ja hankalan tavoiteltavuuden vuoksi heidän osallistumisensa asettaa haasteita. Tiiviillä aikataululla toimittaessa tietoturvatyöpajoihin kutsutaan vain viisihenkinen ehkäisyvälineiden myynnistä vastaava Women’s Healthcare Sales -ryhmä (Liite 3).

5.4 Tietoturvatyöpajojen toteutustapa ja rakenteet

5.4.1 Työpaja koulutustapana

Tietoturvatietoisuuden lisäämiseen ja henkilöstön toiminnan tietoturvapuutteiden kartoittamiseen järjestetään työpajamuotoisia koulutustilaisuuksia, joissa toimin pääsääntöisesti itse tilaisuuksien isäntänä ja kouluttajana. Erikoistapaukset, kuten Espoon henkilöstön koulutus vaativat kollegojeni tukea tiiviin aikataulun ja vaadittavien resurssien vuoksi.

Työpajatyöskentely ei ole kaikkein perinteisin koulutusmuoto, eikä siinä tyydytä VDARS:n koulutuksen kaltaiseen yksipuoliseen kouluttamiseen. VDARS:n koulutuksessa PowerPoint-materiaali vain jaettiin henkilöstölle sähköisesti. NIELIT:n työpajan kaltaisessa työpajatyöskentelyssä diaesitys puolestaan esitetään kokoustiloissa ja työntekijät ovat paikan päällä tilaisuuksissa. Tällaista työpajatyöskentelyä tullaan hyödyntämään kohdeyrityksen tietoturvatyöpajoissa. Työpajoissa on lisäksi monta tietoturvaoppimista edistävää vaihetta ja ne ovat paljon monipuolisempi vaihtoehto pelkkää ohjeistusta sisältävään diaesitykseen verrattuna. Työpajoissa pyritään esityksen läpikäynnin ohessa keskustelemaan avoimesti tietoturvasta ja pohtimaan tietoturvakysymyksiä yhdessä.

Kohdeyrityksessä järjestettävissä tietoturvatyöpajoissa työntekijöitä pyritään aktivoimaan sekä itsenäisten että ryhmässä tehtävien harjoitusten avulla. Näitä harjoituksia hyödynnetään mahdollisimman tehokkaasti tietoturvaoppimisen lisäämiseksi ja toiminnan heikkouksien löytämiseksi. Kaikissa työpajoissa työntekijät vastaavat avoimen kyselyn kaltaisesti työarkkeihin (Liite 4). Näin osallistujille annetaan tehtävänannon asettamissa rajoissa vapaamuotoinen vastausmahdollisuus monivalintalomakkeiden sijaan. Vastaukset annetaan näissä työpajoissa nimettöminä, mutta osasto pyydetään vastausten tarkemman tutkinnan ja analysoinnin vuoksi. Aineiston keräämisen osalta aiheeseen lähestyminen on siis myös varsin erilainen kuin esimerkissä esitellyn Winnipegin kaupungin työntekijöille suunnatussa kyselyssä.

Jokaisessa työpajassa on pääsääntöisesti mukana 10–16 henkilöä siten, että he ovat samasta osastosta tai organisaatioryhmästä. Pienillä ja osastokohtaisilla ryhmillä pyritään luomaan juuri heitä koskevaa keskustelua tietoturvasta, sen haasteista ja eri

toimintatavoista. Järjestettävät työpajat ovat rakenteiltaan hyvin samanlaiset eri kohdeosastojen kohdalla, mutta kestoltaan ja sisällöltään ne eroavat hieman toisistaan.

5.4.2 Työpajojen rakenteet ja sisältö

Toimihenkilöiden työpaja

Turun ja Espoon toimihenkilöiden työpaja on kestoltaan, laajuudeltaan ja sisällöltään niin sanottu normaali työpaja. Taulukossa 2 esitelty työpaja on monipuolinen tapahtuma, jossa käydään tietoturva-asioita läpi osallistuvia aktivoivalla otteella.

Taulukko 2. Toimihenkilöiden työpajan rakenne.

Työpajan rakenne

	Diat	Minuuttia	Minuuttia yht.
Tervetuloa & esittely	6	10	10
Aivoriihi: “Mihin kaikkeen arvokkaaseen informaatioon ja dataan sinulla on pääsy?“	1	10	20
Aivoriihi: “Miten sinä voit tehdä yrityksestä tietoturvallisemman?”	1	10	30
Ryhmätyökonsepti ja ryhmäytyminen	1	5	35
Ryhmätyö	3	30	65
Ryhmien esitykset	1	2 * 5	75
Paluu yhteisosuuteen	-	5	80
Lopetus, seuraavat askeleet ja palaute	1 – 2	10	90

Työpaja aloitetaan tapahtuman ja aiheen esittelyllä. Esittelyosuudessa käydään lyhyesti läpi myös tietoturvakampanjan aikaisempia vaiheita ja yrityksen julkaisemia tietoturvan avainperiaatteita. Osallistujille painotetaan myös yksilön ja tämän toiminnan merkitystä

tietoturva-asioissa. Esittelyosuus on hyvin lyhyt ja sen on tarkoitus palauttaa mieliin aikaisemmin koulutettuja ja opittuja asioita.

Varsinainen työskentelyvaihe on monipuolinen ja se aloitetaan kahdella aivoriihivaiheella. Aivoriihet ovat näissä työpajoissa yksilötyöskentelyvaiheita, joissa pohditaan kymmenen minuutin ajan tietoturvaan liittyviä asioita. Ensimmäisessä aivoriihessä osallistujat pohtivat informaatio- ja dataesimerkkejä, joihin heillä on omassa työssään pääsy eri järjestelmien kautta. Ensimmäisen aivoriihen on tarkoitus saada osallistujat ymmärtämään olemassa olevan tiedon ja ennen kaikkea liiketoiminnan kannalta tärkeän sekä salassa pidettävän tiedon suuren määrän. Toisessa aivoriihivaiheessa osallistujat pohtivat puolestaan niitä asioita, joissa heillä on parannettavaa ajatellen tietoturvallista toimintaa. Molemmissa työvaiheissa osallistujat kirjaavat vastauksensa työarkeille, jotka on havainnollistettu Liitteessä 4.

Yksilötyövaiheiden jälkeen siirrytään ryhmätyövaiheeseen. Ryhmätyövaiheessa osallistujat jakaantuvat kahteen pienryhmään. Molemmat pienryhmät kokoavat työarkeista tiivistelmät heille jaettaville valkotauluille ja keskustelevat aiheesta. Ryhmätyövaiheella on tarkoitus aktivoida osallistujia ja herättää keskustelua tiedon määrästä ja niistä asioista, joissa heillä on vielä parantamisen varaa omassa toiminnassaan. Ryhmätyövaiheen lopuksi pienryhmät viimeistelevät tiivistelmänsä, valitsevat muutaman asiaa, joita he lähtevät heti parantamaan työpajan jälkeen sekä esittelevät lyhyesti tuloksensa toiselle pienryhmälle.

Työpaja päättyy kampanjan seuraavien vaiheiden esittelyyn ja toisen työarkin palautekyselyn täyttämiseen (Liite 4). Palautekyselyssä osallistujat antavat palautetta tapahtuman toimivuudesta ajatellen tietoturvatietoisuuden lisäämistä ja tietoturvatason kehittämistä heidän osastoissaan. Palautekyselyssä annetaan myös mahdollisuus pyytää yhteydenottoa tietoturva-asioihin liittyen.

Kevennetty työpaja

Tietoturvatyöpajoista tehdään myös kevennetty versio, joka on kestoltaan yhden tunnin mittainen (Taulukko 3). Kevennetyssä versiossa työskentelyvaiheiden kestoa on lyhennetty ja itsenäinen työskentelyn määrä on vähennetty vain yhteen aivoriihivaiheeseen. Tässä työpajaversiossa ei pohdita itsenäisesti informaatio- ja

dataesimerkkejä, vaan keskitytään oman toiminnan heikkouksien pohtimiseen ja löytämiseen.

Taulukko 3. Kevennetyn työpajan rakenne.

Työpajan rakenne

	Diat	Minuuttia	Minuuttia yht.
Tervetuloa & esittely	6	10	10
Aivoriihi: “Miten sinä voit tehdä yrityksestä tietoturvallisemman?	1	10	20
Ryhmätyökonsepti ja ryhmäytyminen	1	5	25
Ryhmätyö	2	15	40
Ryhmien esitykset	1	2 * 5	50
Paluu yhteisosuuteen	-	5	55
Lopetus, seuraavat askeleet ja palaute	1 – 2	5	60

Tiiviimpi työpaja laaditaan ensisijaisesti tuotannon työntekijöille. Tuotannon työntekijöillä ei ole laajaa pääsyä yrityksen tietoihin ja yrityksen tietotekniikan käyttö ei ole heillä niin laajaa kuin toimihenkilöillä. Kevennetty versio suunnataan myös IT-osastolle ja myyntihenkilöstölle. IT-osastolle tietoturva-asiat ja -haasteet ovat tutumpia, joten heille tiiviimpi koulutus nähdään riittäväksi. Myyntihenkilöstö on aina liikkeessä ja kiireiden takia myös heille järjestetään lyhyempi työpaja. Vaikka tuotannolle, IT-osastolle ja myyntihenkilöstölle järjestetään kevennetty työpaja, saadaan heiltäkin kerättyä aineistoa tietoturvalliseen toimintaan liittyvien parannuskohteiden löytämiseksi. Kevennetyt työpajat ovat mainittuja tiivistyksiä lukuun ottamatta samanlaisia kuin toimihenkilöille suunnatut normaalit työpajat.

Myyntihenkilöstön työpaja

Myyntihenkilöstön työpaja eroaa merkittävästi normaalista ja kevennetystä työpajasta. Myyntihenkilöt ovat jatkuvassa liikkeessä eri puolilla Suomea, joten heille suunnitellaan erikoistyöpaja. Myyntihenkilöt osallistuvat työpajaan Microsoftin tarjoaman Lync-pikaviestinsovelluksen välityksellä. He eivät ole siis normaaliin tapaan yhdessä koulutustilassa, vaan osallistuvat työpajaan sähköisesti esimerkiksi kotitoimistoiltaan. Lync-tilaisuudessa osallistujille jaetaan esitysmateriaali sovelluksen reaaliaikaisen esitysominaisuuden avulla. Lisäksi varsinainen esittäminen ja muu keskustelu hoidetaan Lyncin verkkopuheluominaisuuden avulla.

Myyntihenkilöstön tietoturvatyöpaja on rakenteeltaan samanlainen kuin normaali toimihenkilöille suunnattu työpaja. Myyntihenkilöiden työpajassa keskitytään kuitenkin enemmän puhumaan tietoturvasta, eivätkä osallistujat varsinaisesti tee tehtäväosuuksia, koska heillä ei ole käytössään työarkkeja tai valkotauluja. Tehtäväosuudet käydään kuitenkin läpi suullisesti ja etenkin tunnistetut tietoturvallisen toiminnan puutteet käydään tarkkaan lävitse. Myyntihenkilöiden työpaja päättyy muiden työpajamuotojen tapaan palautekyselyyn ja sekin suoritetaan suullisesti.

5.5 Työpajojen valmistelut

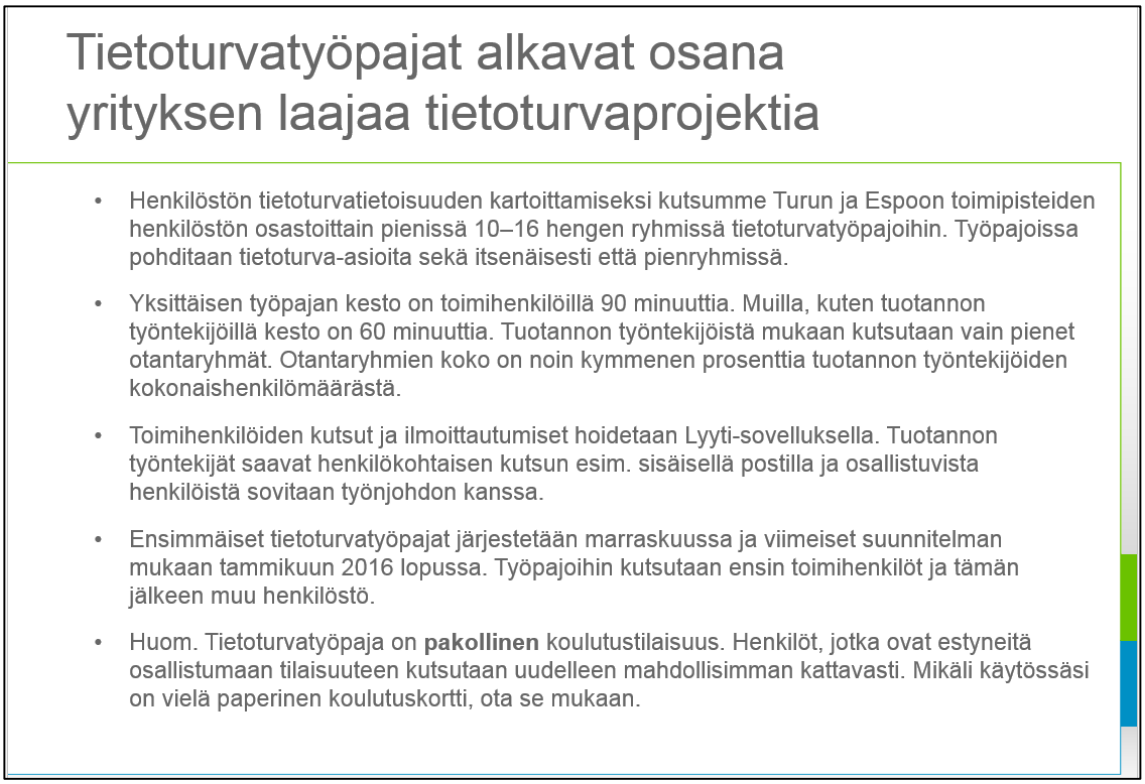
Ennen työpajatyöskentelyn aloittamista tehdään paljon valmistelevia toimenpiteitä. Työpajatyöskentelyä varten sovitetaan jo olemassa olevaa ja kattavaa esitysmateriaalia Suomen henkilöstölle sopivaksi, varataan tarvittavat tilat, tiedotetaan koko henkilöstöä tulevista tilaisuuksista, jaetaan työntekijät työpajaryhmiin ja laaditaan kutsut tuleviin tilaisuuksiin.

Tietoturvatyöpajoissa käytetään havainnollistamisen helpottamiseksi PowerPoint-esitystä. Esitystä laadittaessa hyödynnetään yrityksen globaalia PowerPoint-pohjamateriaalia. Vaikka yrityksen korkeimmat tietoturvatahot kehottavat käyttämään kyseistä pohjaa, esitystä kuitenkin muokataan Suomessa toimivan henkilöstön kannalta sopivaksi. Tämä tarkoittaa etenkin sitä, että koulutusmateriaalin muokkaamisessa otetaan huomioon kaikki kohdeosastot. Englantia äidinkielenään puhuville työntekijöille laaditaan englanninkielinen versio ja tuotannon, IT-osaston sekä myynnin henkilöstölle valmistellaan omat versionsa teknisine lisäjärjestelyineen.

Koulutusmateriaalin lisäksi valmistelua vaativat myös aineiston keräämiseen käytettävät työarkit (Liite 4). Työarkit pidetään yksinkertaisina, selkeinä ja mahdollisimman samanlaisina koko henkilöstön osalta. Muutamalle englantia puhuvalle työntekijälle laaditaan englanninkieliset työarkit, jotka ovat sisällöltään täysin samanlaiset kuin normaalit suomenkieliset työarkit.

Esitysmateriaalin lisäksi iso osa työpajojen valmistelua ovat tilavaraukset. Työpajoja varten varataan Turun toimipisteessä yksi neuvottelutila pysyvällä varauksella, joka kestää koko projektin ajan. Näin saadaan pysyvä paikka koulutustilaisuuksille. Espoon toimistolla tilavaraukset tehdään myös tiettyihin neuvottelutiloihin.

Tulevista tietoturvatyöpajoista julkaistaan koko henkilöstön luettaviin tiedotteita eri tiedotuskanavia käyttäen. Henkilöstöä tiedotetaan yrityksen intranetissä sekä yrityksen toimipisteiden info-televisioissa. Kuvassa 5 on yrityksen henkilöstölle julkaistu tiedote tietoturvatyöpajoista. Tiedottamisella pyritään vähentämään tarkentavien kysymysten määrää, antamaan ennakkotietoja tapahtumasta ja etenkin auttaa toimihenkilöitä sovittamaan tulevat tapahtumat omiin aikatauluihinsa.



Kuva 5. Tiedote tulevista tietoturvatyöpajoista.

Tiedottamisen jälkeen henkilökunta jaetaan 10–16 hengen ryhmiin siten, että jokaisessa työpajassa on mukana pääosin saman osaston henkilöitä. Kaiken kaikkiaan työpajaryhmiä muodostetaan alustavasti 40 ja ne jakautuvat

- 34 normaaliin toimihenkilöryhmään
- kahteen tuotannon ryhmään
- kahteen vuokratyöntekijöiden ryhmään
- yhteen IT-osaston ryhmään
- yhteen myyntihenkilöstön ryhmään.

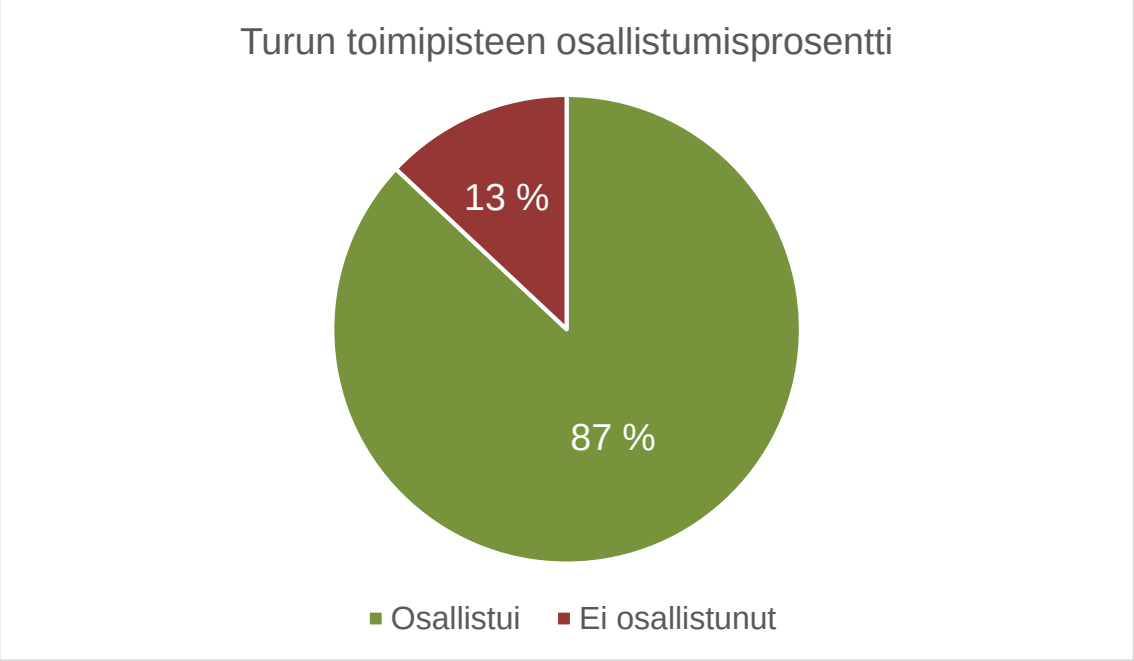
Ryhmäjaon työpajaryhmät kutsutaan työpajoihin käyttäen sekä sähköisiä ja perinteisiä paperikutsuja. Sähköiset kutsut lähetetään kaikille työntekijöille, joilla on mahdollisuus vastaanottaa niitä omaan työsähköpostiinsa. Kaikilla työntekijöillä tätä mahdollisuutta ei ole, joten heille lähetetään paperikutsut. Yrityksen suuren henkilöstömäärän myös kutsuja luodaan paljon. Sähköiset kutsut laaditaan tapahtumien järjestämisen tueksi kehitetyn Lyyti-verkkopalvelun avulla. Ulkoasultaan sähköisten kutsujen kanssa identtiset paperikutsut laaditaan tietokoneella ja lähetetään yrityksen sisäistä postia hyödyntäen.

6 TIETOTURVATYÖPAJOJEN TULOKSET

6.1 Osallistumisprosentit

6.1.1 Turun tuotantolaitos

Turun tuotantolaitokselta työpajoihin kutsuttiin kaiken kaikkiaan 378 työntekijää, joista 329 osallistui tietoturvatyöpajoihin. Kuviossa 3 on esitetty Turun toimipisteen osallistujamäärä prosenttimuodossa.

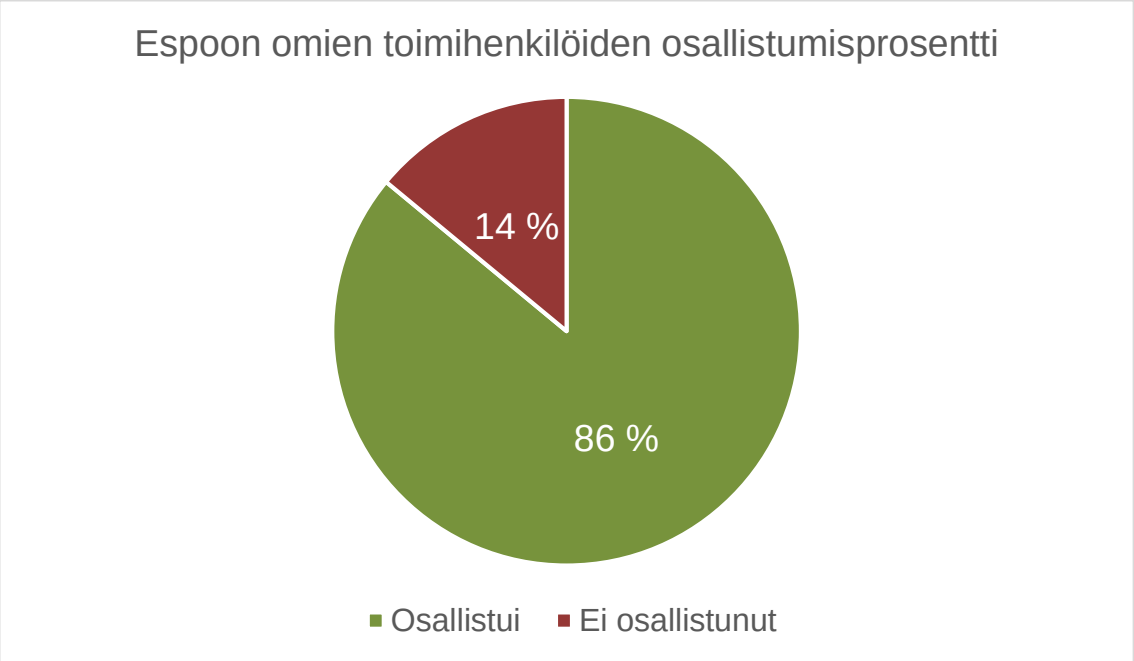


Kuvio 3. Turun toimipisteen osallistumisprosentti.

Tavoitteeksi asetetun 80 %:n tavoite täytettiin ja suurin osa saatiin osallistumaan tietoturvatyöpajatyöskentelyyn. Vain pieni osa kutsutuista jäi pois liikematkojen, sairastumisten ja muiden esteiden vuoksi.

6.1.2 Espoon toimisto

Espoon toimipisteestä työpajoihin kutsuttiin yrityksen omia toimihenkilöitä ja vuokratyöntekijöitä. Kaiken kaikkiaan Espoosta kutsuttiin mukaan 91 yrityksen omaa työntekijää, joista 78 osallistui tietoturvatyöpajoihin. Omien toimihenkilöiden osallistumisen osalta myös Espoossa päästiin tavoitteisiin, eikä poisjääntejä ollut lopulta kuin alle viidennes (Kuvio 4).



Kuvio 4. Espoon omien toimihenkilöiden osallistumisprosentti.

Espoon toimiston vuokratyöntekijöistä tietoturvatyöpajoihin kutsuttiin 49 työntekijää. Osallistumisen osalta jäätiin tavoitteesta ja osallistujia oli yhteensä vain 28, joten osallistumisprosentti oli vain hieman yli 50. Kuviossa 5 on esitetty Espoon toimistolta kutsuttujen vuokratyöntekijöiden osallistumisprosentti.

Kuvio 5. Espoon vuokratyöntekijöiden osallistumisprosentti.

Espoon vuokratyöntekijöille ei ehditty tiiviin aikataulun vuoksi järjestää uusia työpajoja, mikä näkyy osallistumisprosentissa selkeästi. Alhaiseksi jääneestä osallistumismäärästä huolimatta vuokratyöntekijöiden vähäistäkin osallistumista työpajatyöskentelyyn pidettiin erittäin tärkeänä asiana.

6.1.3 Myyntihenkilöstö

Myyntihenkilöstöstä työpajoihin kutsuttiin vain yksi viiden hengen ryhmä aivan projektin lopuksi. Viidestä kutsutusta myyntihenkilöstä kaikki osallistuivat tietoturvatyöpajaan. Kaikki myyntihenkilöt on tarkoitus saada mukaan tietoturvatyöpajoihin, mutta tähän opinnäytetyöhön sisältyy vain Women’s Health Care -myyntiryhmän osallistuminen. Muun myyntihenkilöstön tietoturvatyöpajat järjestetään tulevaisuudessa kohdeyrityksen toimesta.

6.1.4 Koko Suomen henkilöstö

Kohdeyrityksen osalta tietoturvatyöpajoihin kutsuttiin kaiken kaikkiaan 523 työntekijää yrityksen Suomessa työskentelevästä yli kahdeksansadan ihmisen henkilöstöstä. Tavoitteeksi asetettu kahdeksankymmenen prosentin osallistujatavoite täytettiin suomen osalta, sillä 440 työntekijää (84 %) kutsutuista osallistui tietoturvatyöpajoihin. Kuviossa 6 on esitetty koko Suomen henkilöstön osallistuminen työpajatyöskentelyyn.

Kuvio 6. Yrityksen koko Suomen henkilöstön osallistumisprosentti.

Kaikkia Suomessa työskenteleviä yrityksen työntekijöitä – kuten esimerkiksi jokaista tuotannon työntekijää – ei kutsuttu mukaan työpajatyöskentelyyn ylimmän johdon ja tietoturvavastaavien toiveesta. Lisäksi seuraavista kutsutuista osastoista ei estymisten takia saatu osallistujia työpajoihin:

- Global Data Sciences & Analytics (Espoo)
- Human Resources (Espoo)
- Medical Affairs (Turku)
- Samson Special Items (Espoo)
- Study Management (Turku).

Nämä pois jääneet osastot ovat henkilömääriltään todella pieniä. Näin ollen niiden vaikutus kokonaisosallistujamääräänkin on minimaalinen.

Suurin osa kutsutusta henkilöstöstä saatiin mukaan tietoturvatyöpajoihin ja asetettuihin osallistujatavoitteisiin päästiin. Kaiken kaikkiaan lopullista osallistujaprosenttia voidaan pitää erinomaisena ottaen huomioon työskentelyn suuren henkilöstömäärän ja monen eri osaston kanssa kahdella eri paikkakunnalla.

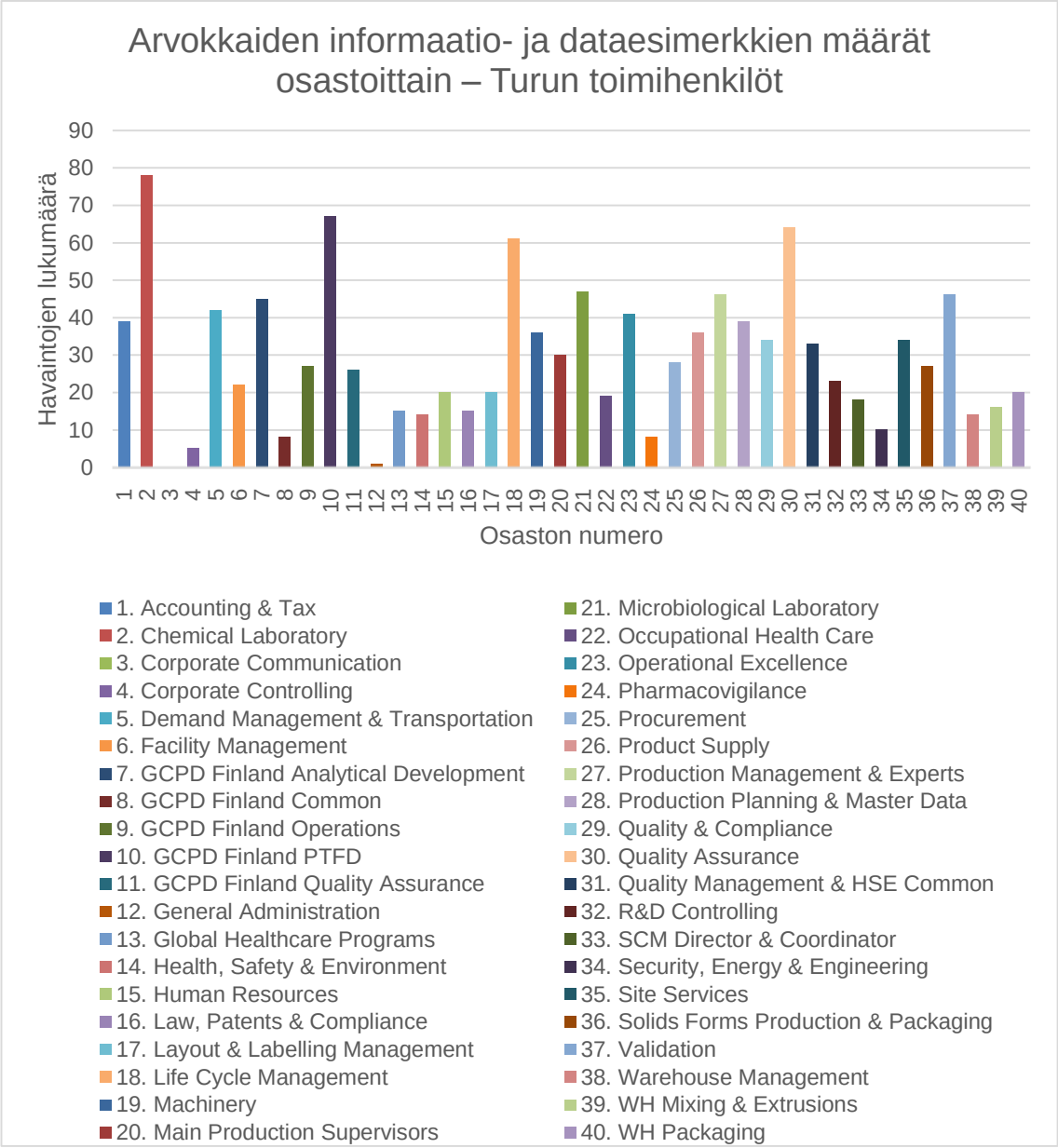
6.2 Henkilöstön tietoturvallisuuden kehitys

Tietoturvatyöpajoilla pyrittiin lähtökohtaisesti lisäämään henkilöstön tietoturvatietoisuutta ja -osaamista. Työpajoja käytettiin koulutustilaisuuksina ja pyrittiin näin saamaan aikaan välitöntä vaikutusta henkilöstön käyttäytymiseen ja viemään sitä tietoturvallisempaan suuntaan. Tietoturvakehityksen välitöntä edistymistä mitattiin ensisijaisesti Liitteen 4 toisen työarkin palautekyselyn avulla. Palautekyselyssä pyydettiin osallistujien näkemystä siihen, kuinka hyvin työpajatyöskentely lisäsi heidän tietoturvatietoisuuttaan ja osaamistaan jatkoa ajatellen.

Palautekyselyn ohella tietoturvatyöpajoissa käytettiin Liitteen 4 ensimmäisessä työarkissa esitettyä itsenäisen työskentelyn vaihetta. Tässä työskentelyvaiheessa osallistujat saivat pohtia eri esimerkkejä arvokkaasta informaatiosta ja datasta. Työskentelyvaiheen tarkoituksena oli saada työntekijät ymmärtämään arvokkaan tiedon määrä ja pohtimaan tietojen suojaamisen tärkeyttä. Turun, Espoon ja myynnin osastojen pohtimia esimerkkejä kertyi vaihtelevasti osin osaston koosta ja toimenkuvasta riippuen.

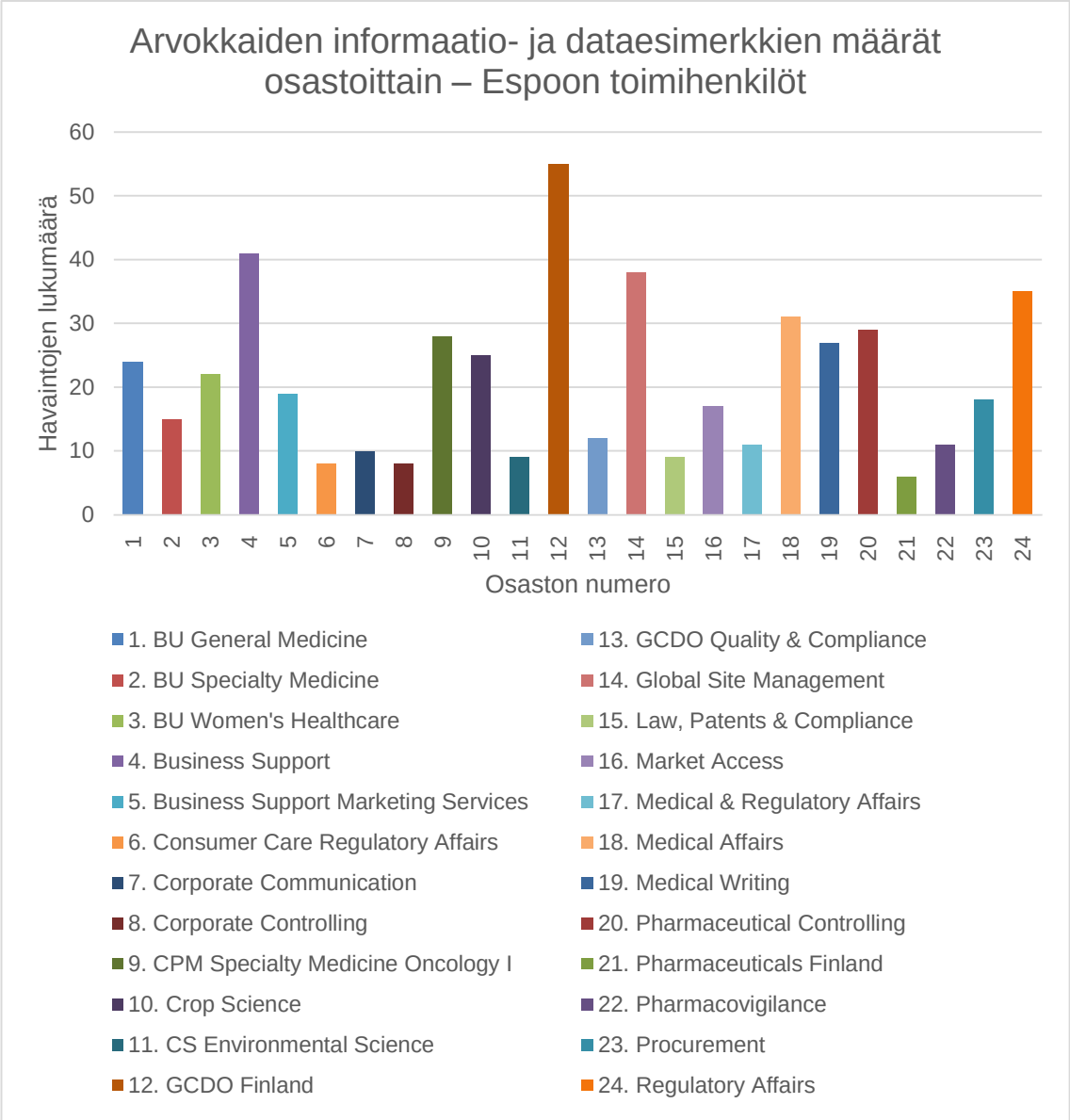
Tulosten esittämisessä ja havainnollistamisessa käytetään pääsääntöisesti osastojen englanninkielisiä nimiä ja lyhenteitä yrityksen kansainvälisyyden vuoksi. Kaikkien osastojen suomenkieliset selitteet löytyvät Liitteissä 1, 2 ja 3 esitetyistä osallistuvien osastojen listauksista.

Turun toimihenkilöosastojen pohtimia esimerkkejä on esitetty Kuviossa 7. Arvokkaan tiedon määrä osoittautui suureksi etenkin kemiallisen laboratorion, PTFD-tuotekehityksen, tuote- ja prosessielinkaarien hallinnan (Life Cycle Management) sekä laadunvarmistuksen osastoissa. Vähiten esimerkkejä kirjasivat pääsääntöisesti pienet osastot, kuten yleishallinto (General Administration) ja viestintä (Corporate Communication).



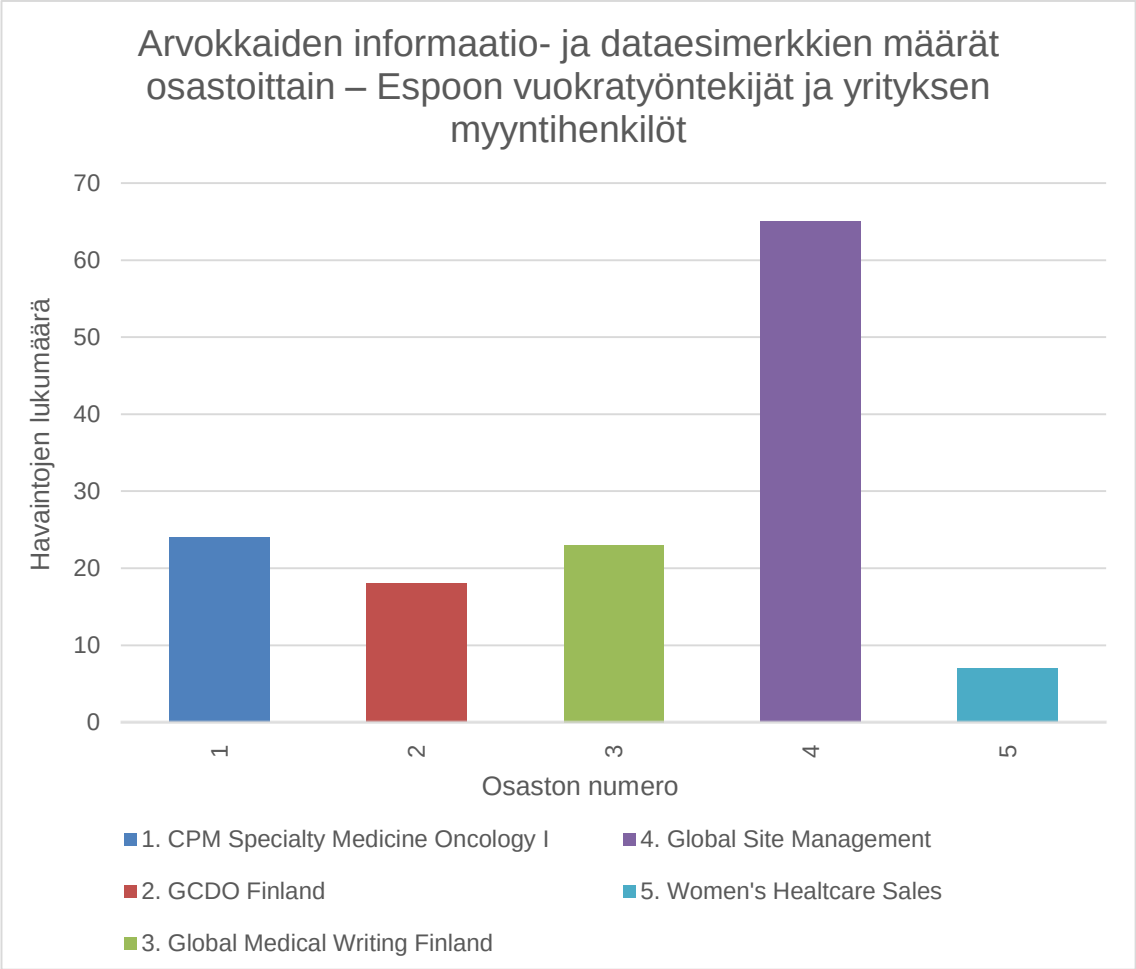
Kuvio 7. Turun toimihenkilöiden pohtimien arvokkaiden tietoesimerkkien määrät.

Espoon toimistolla työskentelevien yrityksen omien toimihenkilöiden pohtimia esimerkkejä on koottu Kuvioon 8. Espoon osalta eniten esimerkkejä listasivat kliinisen kehityksen yksikön (GCDO Finland) työntekijät. Muiden osastojen osalta määrät ovat hyvin vaihtelevia. Jokainen osasto kuitenkin tunnisti omasta työstään esimerkkejä yrityksen kannalta tärkeästä ja arvokkaasta tiedosta, joita tulee käsitellä huolellisesti.



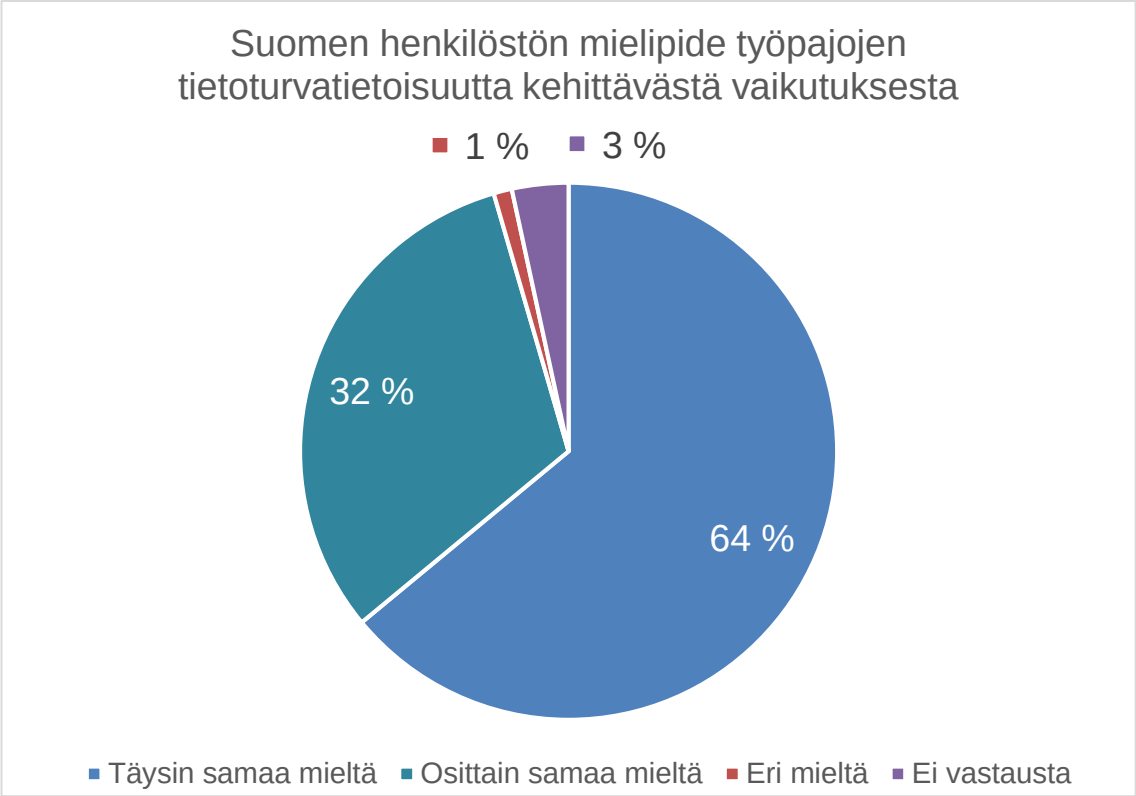
Kuvio 8. Espoon toimihenkilöiden pohtimien arvokkaiden tietoesimerkkien määrät.

Vuokra- ja myyntityöntekijöistä selkeästi eniten esimerkkejä arvokkaasta tiedosta listasivat Global Site Managementin työntekijät. Muut vuokratyöntekijäosastot listasivat esimerkkejä lähes yhtä paljon toisiinsa nähden. Vähiten tietoesimerkkejä tuli pieneltä Women's Healthcare Sales -myynnin ryhmältä. Vuokratyöntekijöiden ja myynnin yhden osallistujaryhmän pohtimat informaatio- ja dataesimerkit on koottu Kuvioon 9.



Kuvio 9. Vuokra- ja myyntityöntekijöiden pohtimien arvokkaiden tietoesimerkkien määrät.

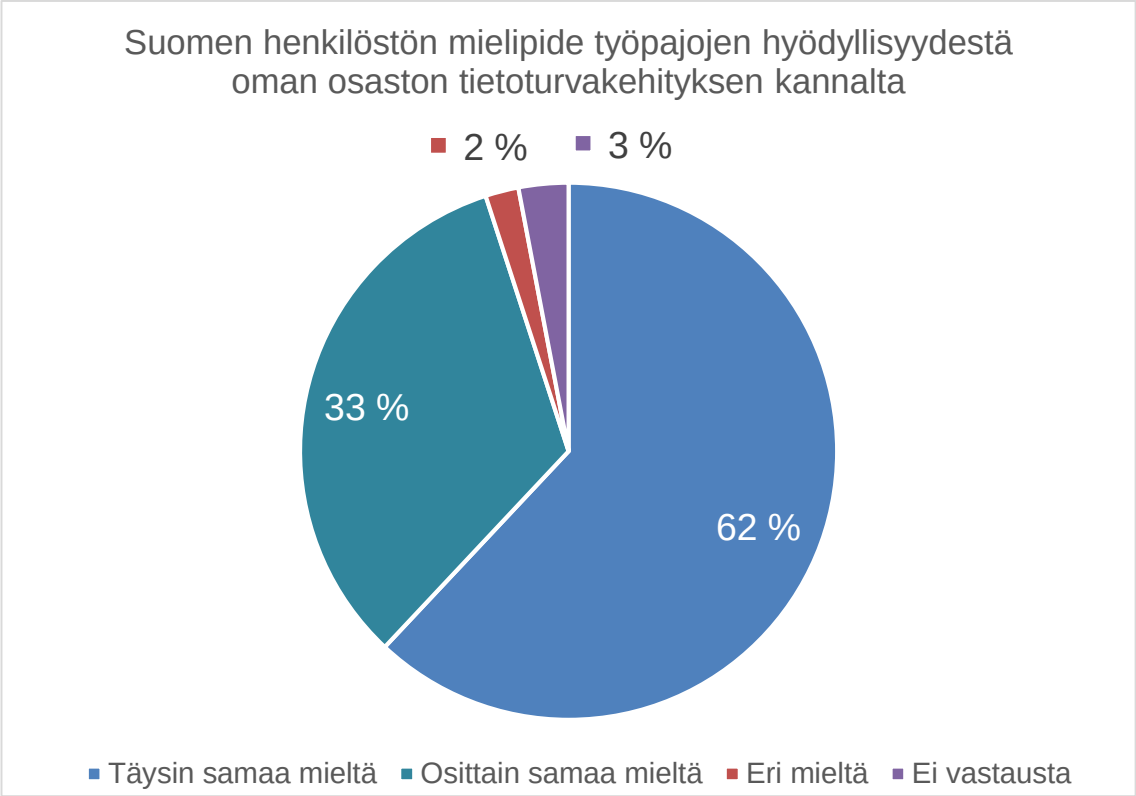
Palautekyselyn osalta tärkeimpänä pidettiin koko Suomen osallistujien mielipidettä tietoturvatyöpajojen toimivuudesta tietoturvatietoisuuden ja -osaamisen välittömänä kehittäjänä. Yrityksen Suomen henkilöstön mielipide työpajojen kehittävästä vaikutuksesta tietoturvatietoisuuden tasoon on esitetty Kuviossa 10.



Kuvio 10. Suomen henkilöstön mielipide työpajojen tietoturvatietoisuutta kehittävästä vaikutuksesta.

Suurin osa osallistuneista työntekijöistä oli täysin tai osittain samaa mieltä siitä, että tietoturvatyöpajat kehittivät tietoturvatietoisuutta heidän omassa työpajaryhmässään ja osastossaan. Vain pieni osa osallistuneesta henkilöstöstä piti työpajoja toimimattomina tietoturvatietoisuuden lisäämistä ajatellen. Vastaamatta jättäneiden lukumäärä oli myös hyvin vähäinen.

Palautteen toisessa osassa osallistujilta pyydettiin mielipidettä tietoturvatyöpajojen hyödyllisyydestä ajatellen osaston tietoturvatason kokonaisvaltaista nostamista. Kuviossa 11 on esitetty mielipiteiden jakautuminen hyödyllisyyden osalta.



Kuvio 11. Suomen henkilöstön mielipide työpajojen hyödyllisyydestä oman osaston tietoturvakehityksen kannalta.

Tietoturvakehityksellisen hyödyllisyyden osalta mielipiteet jakautuivat hyvin samalla tavalla kuin tietoturvatietoisuuden lisääntymistä koskevat mielipiteet. Suurin osa henkilöstöstä piti tietoturvatyöpajoja myös tietoturvakehitystä ajatellen täysin tai osittain onnistuneina tilaisuuksina. Hyvin harva piti työpajoja oman osaston tietoturvan parantamisen kannalta toimimattomina tai jätti kokonaan vastaamatta.

Palauteosiossa oli erikseen myös mahdollista pyytää IT-osaston yhteydenottoa tietoturvakysymyksiin liittyen. Kaiken kaikkiaan 30 henkilöä pyysi yhteydenottoa. Yhteydenotot käsitellään yrityksen toimesta erikseen ja jätetään tämän opinnäytetyön ulkopuolelle.

Tietoturvatietoisuutta ja -osaamista pystyttiin lisäämään tehokkaasti työpajojen aikana. Lisäksi työntekijöiden pohdittua heidän omassa työssään käsittelemää arvokasta tietoa saatiin aikaan keskustelua ja ymmärrystä turvallisen toiminnan ja huolellisen tietojenkäsittelyn välttämättömyydestä.

6.3 Henkilöstön tietoturvallisen toiminnan parannuskohteet

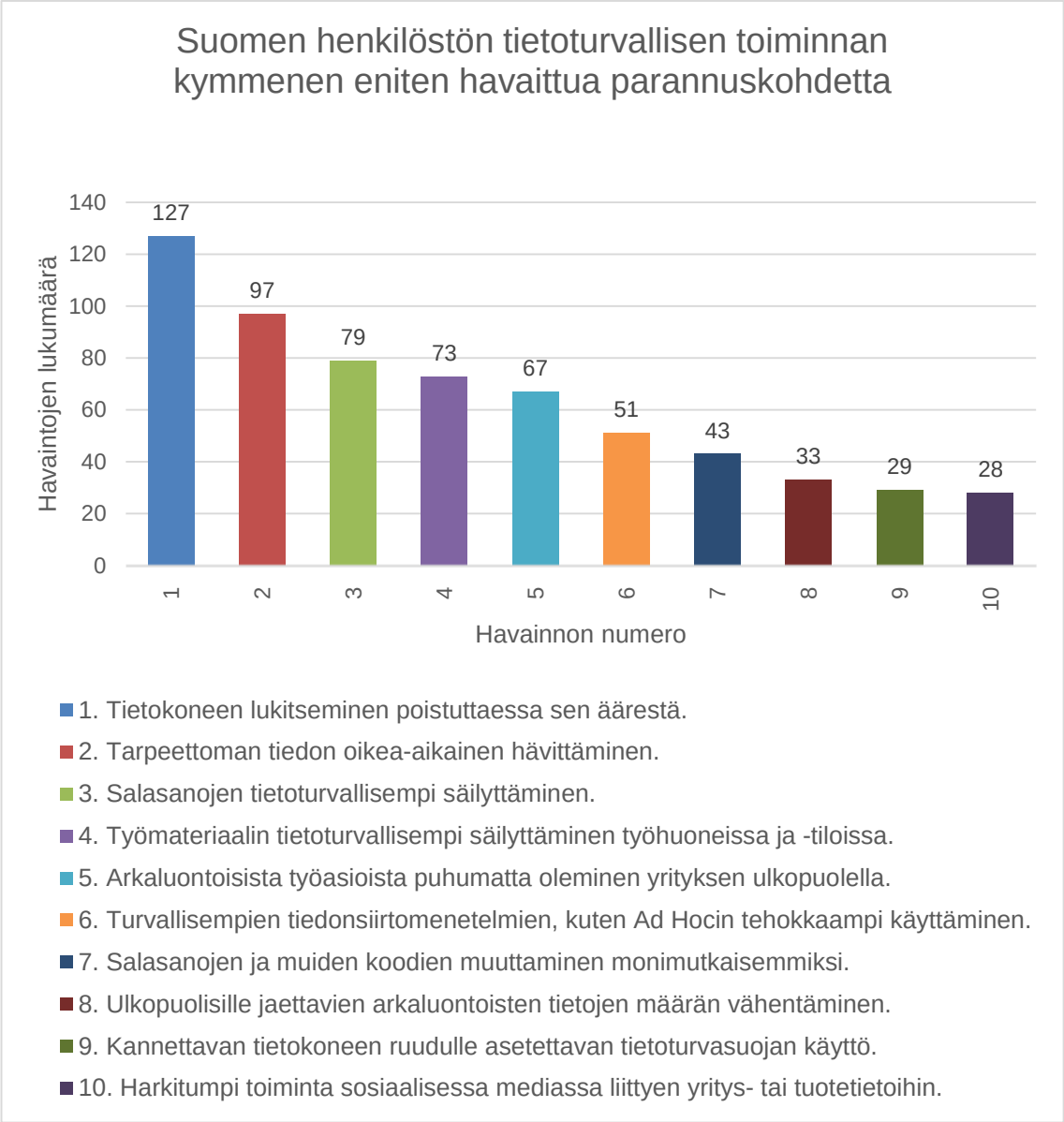
Tietoturvatyöpajoilla pyrittiin välittömän vaikutuksen lisäksi selvittämään myös henkilöstön toiminnan kriittisimmät ja yleisimmät tietoturvapuutteet. Tietoturvapuutteiden kartoittamisessa ei haluttu lähteä syyllistämään henkilöstöä. Tämän takia virheellisen ja vääränlaisen toiminnan sijaan henkilöstöä kehotettiin listaamaan Liitteen 4 toiselle työarkille niitä toimenpiteitä, joilla he voivat positiivisesti vaikuttaa tietoturvakehitykseen.

Turun toimihenkilöiden ja tuotannon työntekijöiden osalta parannuskohteita kertyi runsaasti varsinkin suuren henkilöstö- ja osastomäärän vuoksi. Turun henkilöstön toiminnassa havaittiin puutteita kaikkein eniten tietokoneiden lukitsemisessa poistuttaessa sen äärestä. Useimmiten esiintyneitä parannuskohteita olivat lisäksi tarpeettoman tiedon hävittäminen, salasanojen turvallinen säilyttäminen, työmateriaalin säilytys muualla kuin työpöydällä sekä työasioista puhumatta oleminen julkisilla paikoilla.

Espoon toimihenkilöiden osalta parantamisen varaa havaittiin eniten siinä, että julkisilla paikoilla puhutaan työasioista. Useimmin esiintyneitä parannuskohteita olivat myös työpöydän siisteys, tietokoneen lukitseminen poistuttaessa sen äärestä, tietoturvallisempien tiedonvälitysmenetelmien käyttäminen sekä kannettavan tietokoneen ruudulle asetettavan tietoturvasuojan hankkiminen IT-osaston kautta.

Vuokratyöntekijöiden osalta kriittisimmät parannuskohteet olivat julkisilla paikoilla toimiminen, salasanojen turvallisempi säilyttäminen, tietokoneen näytön tietoturvasuojan käyttäminen sekä työasioista puhumatta oleminen yleisillä paikoilla ja ulkopuolisten kanssa. Yrityksen myyntihenkilöstöstä osallistunut ryhmä pohti sähköpostiviestien salaamistoiminnon aktiivisemman käyttämisen olevan ainoa parannuskohde, johon tulee jatkossa kiinnittää enemmän huomiota.

Koko yrityksen Suomen henkilöstön osalta parannuskohteista kriittisimmät koottiin kokonaiskuvan ja kaikkein tärkeimpien havaintojen löytämiseksi. Erilaisia parannuskohteita löydettiin koko Suomen henkilöstön osalta kaiken kaikkiaan 164 kappaletta. Näistä yli sadasta havainnosta kymmenen tärkeintä ja eniten havaittua kohdetta on havainnollistettu Kuviossa 12. Nämä havainnot ovat ne kohteet, joita tulisi ensisijaisesti kehittää henkilöstön toiminnassa.



Kuvio 12. Suomen henkilöstön tietoturvallisen toiminnan kymmenen eniten havaittua parannuskohdetta.

Eniten henkilöstön vastausten perusteella on parannettavaa tietokoneen lukitsemisessa. Tiedon säilyttämisessä ja hävittämisessä sekä salasanojen hallinnoinnissa on myös kehitettävää. Henkilöstön vastauksista käy ilmi myös tietoturvalliseen viestintään ja yrityksen ulkopuolella tapahtuvaan käyttäytymiseen liittyvät puutteet. Tietoturvallisten tiedonsiirtomenetelmien – kuten yrityksen käyttämän Ad Hoc -tiedostonsiirtopalvelun – käyttämisen lisäämisessä on myös parannettavaa. Yrityksen käyttämässä Ad Hoc -tiedostonsiirtopalvelussa hyödynnetään erillistä viestipalvelinta, josta vastaanottaja

hakee tiedon itse sähköpostiaan hyödyntäen. Ad Hoc -viestipalvelimella on aina käytössä viestin salaus ja viestitapahtumat ovat paremmin valvottavissa kuin perinteisessä sähköpostiliikenteessä.

Hyödyntämällä tietoturvatyöpajoja tehokkaasti saatiin selville runsaasti kohdeyrityksen tietoturvakehityksen kannalta tärkeitä asioita. Työpajat olivat henkilöstön mielestä hyvä tapa kehittää tietoturvaa ja pohtia tietoturva-asioita yhdessä. Lisäksi tutkimuksen tuloksena löydetyt henkilöstön tietoturvallisen toiminnan parannuskohteet auttavat yritystä jatkossa suunnittelemaan ja toteuttamaan toimenpiteitä tietoturvatason nostamiseksi.

7 SUOSITUKSET HENKILÖSTÖN TIETOTURVATASON PARANTAMISEKSI

Tietoturvatyöpajojen tuloksien huolellisen läpikäynnin jälkeen yrityksen tulee pohtia tietoturvakehityksen seuraavia askelia. Aktiivisuus tietoturva-asioissa ja henkilöstön tietoturvaosaamisen jatkuva kehittäminen eri menetelmin on tärkeää yrityksen kokonaistietoturvan tason kannalta. Seuraavassa on esitelty suositusten muodossa mahdollisia työpajojen jälkeisiä toimenpiteitä tietoturvakehityksen jatkamiseksi.

7.1 Tulosten jakaminen osastoille

Tietoturvatyöpajoista kootut tulokset voidaan jakaa suoraan osastoille. Näin osastot voivat itsenäisesti pohtia kehittämisen kohteita. Tulosten esittäminen virheellisenä toimintana suoraan osastojen työntekijöille voi tuntua heistä varsin syyllistävältä. Vaikka tulokset tuleekin välittää jollain tavalla henkilöstölle, sen toteuttamiseen voidaan pohtia vaihtoehtoisia ratkaisuja. Osastojen itsenäisen pohdinnan tapauksessa esimiesten rooli korostuu. Esimiesten on otettava esimerkillinen asenne ja suhtauduttava havaittuihin parannuskohteisiin vakavasti. Tulosten jakamisen jälkeen osastot voivat itse seurata kehitystään. Lisäksi jaettavat tulokset pysyvät muistilappuna myös jatkossa ja niihin on helppo palata.

Tietoturvan kannalta parannettavia kohteita on osastoissa varmasti useampiakin kuin ne, jotka havaittiin työpajojen tiivistetyistä tuloksista. On kuitenkin hyvä aloittaa pienestä määrästä havaintoja, jolloin työmäärä pysyy kohtalaisena ja niiden läpikäynti on osastoille mielekästä.

7.2 Jatkuva kouluttaminen ja kartoittaminen

Yrityksen on hyvä kouluttaa henkilöstöään tietoturva-asioista myös jatkossa. Perinteisten koulutusmenetelmien lisäksi näiden tietoturvatyöpajojen kaltaiset koulutustilaisuudet ovat erinomaisia vaihtoehtoja. Jatkossa järjestettävissä tietoturvakoulutuksissa tulee pohtia käytännön esimerkkien ja harjoitteiden mukaan ottamista. Konkreettiset esimerkit tietoturvauhista tai aikaisemmin tapahtuneista

tietoturvarikkomuksista tukevat tietoturvaoppimista ja koulutustilaisuuksista saadaan mielekkäämpiä osallistuvalle henkilöstölle.

Kouluttamisen lisäksi jatkuva tietoturvaosaamisen kartoittaminen on tärkeää. Tietoturvataitojen mittaamiseenkin on perinteisten paperikyselyiden tilalle muita vaihtoehtoja. Tärkeintä on pysyä tilanteen tasalla ja tunnistaa henkilöstön toiminnassa olevat tietoturvaheikkoudet ajoissa.

7.3 Tiedottamiseen panostaminen

Tiedottamisen merkitystä ei voida väheksyä. Tietoturvatyöpajojenkin tulosten perusteella henkilöstö kaipaa enemmän tiedottamista tietoturva-asioista. He eivät välttämättä tiedä mikä on tietoturvallisesti oikeaa toimintaa ja mikä puolestaan ei. Näiden asioiden selvittämiseen riittävät usein yksinkertaisetkin toistuvat tiedotteet.

Konkreettinen esimerkki tiedottamisen puutteesta on työntekijöiden tietämättömyys kohdeyrityksen käyttöönottamasta salasanojen hallintaohjelmasta. Hallintaohjelmaan saa listattua omia salasanoja ja tunnuksia muistiin yhden pääsalasanan taakse. Kyseisen ohjelman on jo pidemmän aikaa saanut IT-osastolta. Henkilöstö ei kuitenkaan ollut tietoinen ohjelmasta ja vasta tietoturvatyöpajoissa heräsi laajempaa keskustelua aiheesta. Salasanan hallintaohjelman puuttuminen käyttäjiltä on yksi syy siihen, että salasanoja kirjataan työpisteellä oleviin vihkoihin ja muistilappuihin.

7.4 Positiivinen kannustaminen

Henkilöstön tietoturvakehityksessä on tärkeää suhtautua tietoturvaan ja sen haasteisiin positiivisesti kannustavalla asenteella. Henkilöstön mielestä tietoturva-asiat ovat usein jo lähtökohtaisesti vastenmielisiä. Uudet tietoturvakäytännöt tai -vaatimukset nähdään usein työtä hidastavina tekijöinä ja näin niihin suhtaudutaan huonolla asenteella.

Tietoturvatyöpajat osoittivat sen, että etenkin kouluttajan positiivinen asenne edistää oppimista ja auttaa luomaan keskustelua aiheesta. Tietoturvaan on suhtauduttava vakavasti, mutta henkilöstön kouluttamisen ei tarvitse olla väkinäistä ja monta tuntia kestävää luennointia. Kannustavat ja vaihtelevat koulutusmenetelmät ovat omiaan tempaamaan yleisön mukaan koulutukseen ja tietoturvakehitykseen.

8 POHDINTA

8.1 Tavoitteiden täyttyminen

Koko tutkimuksen tavoitteisiin kuului kolme päätavoitetta. Ensisijaisena tavoitteena oli yrityksen Suomessa työskentelevän henkilöstön kouluttaminen tietoturvatyöpajojen avulla. Toinen päätavoite oli löytää tietoturvatyöpajojen avulla henkilöstön tietoturvallisen toiminnan kehityskohteita. Viimeisenä tavoitteena oli listata kehitysehdotuksia liittyen siihen, miten yritys voisi kehittää henkilöstötietoturvaansa työpajatyöskentelyn jälkeen. Osallistumistavoitteesta muodostui oma alitavoitteensa, jonka mukaan 80 % kutsutuista työntekijöistä pyrittiin saamaan paikalle.

Tarvittava määrä tietoturvatyöpajoja saatiin järjestettyä ja henkilöstö saatiin tehokkaasti koulutettua. Kaiken kaikkiaan tilaisuuksia järjestettiin 48. Kutsuttujen osalta osallistumisprosentti oli loppujen lopuksi 84 %, joten kovaan osallistumistavoitteeseen päästiin. Tämä onnistui tehokkailla koulutusjärjestelyillä, joihin kuului ennen kaikkea uusien tietoturvatyöpajaryhmien ja -tilaisuuksien hallintaa.

Henkilöstön toiminnasta löydettiin kattavasti erilaisia kehityskohteita tietoturvaan liittyen. Tärkeimmät ja useimmiten esiintyneet parannuskohteet listattiin yrityksen jatkotoimenpiteiden suunnittelun tueksi. Kaiken kaikkiaan parannuskohteita löydettiin runsaasti ja tutkimuksen alussa asetettuun tavoitteeseen päästiin.

Havaintojen perusteella toimeksiantaja voi pohtia tulevaisuuden toimenpiteitään henkilöstötietoturvaan liittyen. Opinnäytteen viimeisen tavoitteen täyttämiseksi työpajatyöskentelyn jälkeen tehdyn pohdinnan perusteella listattiin ehdotuksia tietoturvatason kehittämiseksi. Listatut ehdotukset perustuvat kerätyn tutkimusaineiston ohella myös työpajoissa tehtyihin havaintoihin ja työpajaryhmien kanssa käytyihin keskusteluihin.

Tutkimukselle asetetut tavoitteet olivat korkealla ja lukuisat eri haasteet hankaloittivat niihin pääsemistä. Loppujen lopuksi kaikkiin tavoitteisiin kuitenkin päästiin ja lopputulokseen voidaan olla tyytyväisiä.

8.2 Haasteet

Työpajaprojekti oli kokonaisuudessaan onnistunut, mutta matkan varrella eteen tuli monenlaisia haasteita. Haasteita oli ennen varsinaisen työpajatyöskentelyn aloittamista, sen aikana ja sen jälkeenkin.

Haasteita oli jo ennen työpajatyöskentelyn aloittamista. Ensimmäisen suuren haasteen asettivat suuri henkilöstömäärä ja tiivis aikataulu. Tiiviin aikataulun vuoksi työpajoja pidettiin useana päivänä viikossa sekä aamu- että iltapäivisin. Suuri henkilöstömäärä tiesi myös suurta määrää ryhmiä. Sopivien 10–16 hengen ryhmien muodostaminen lukuisista eri osastoista oli ajoittain hankalaa. Lisähaasteen toi se, ettei tuotannon henkilöstöstä osallistuvia työntekijöitä voinut valita sattumanvaraisesti. Tuotannon henkilöstöä kutsuttaessa oli otettava huomioon etenkin vuorotyön ja jatkuvan tuotannon asettamat haasteet.

Ryhmät kutsuttiin samaan tilaan, johon tehtiin koko projektin kestävä varaus. Saman neuvottelutilan pitkäaikainen varaaminen samoihin ajankohtiin eri viikkoina vaati myös selvittelyä ja sopimista muiden työntekijöiden kanssa. Turun toimipisteen lisäksi tilavarauksia tehtiin myös Espoon toimistolle, mikä oli oma haasteensa. Hieman Turun toiminnasta poikkeavat käytännöt ja toimintaympäristöt vaativat myös lisäselvittelyä.

Haasteita tuli eteen myös työpajojen aikana ja niiden jälkeen. Työpajaprojektin alkutaipaleella tehtyjä tilavaruksia jouduttiin siirtämään tärkeiden kokousten, vierailijatapahtumien ja viranomaistarkastuksiin liittyvien tilaisuuksien tieltä toisiin neuvottelutiloihin. Tilavaihdoksia tapahtui lyhyelläkin varoitusajalla, ja kaikkien jo kutsuttujen työntekijöiden uudelleeninformointi oli ajoittain todella hektistä.

Tavoitteena ennen työpajatyöskentelyä oli, että osallistumisprosentti saadaan yli 80 %:iin. Tämän vuoksi haasteeksi muodostui poisjääneiden henkilöiden uudelleenkutsuminen. Poissaolot vaativat uusien ryhmien muodostamista sekä uusia tilavarauksia ja ne toivat mukanaan ajankäyttöön liittyviä haasteita. Ylimääräisiä työpajoja järjestettiin kaikkiaan kahdeksan. Espoon toimiston runsaiden poissaolojen vuoksi oli välttämätöntä järjestää siellä kokonaan uusi työpajapäivä.

Työpajojen päätyttyä tutkimusaineistoa oli paljon ja sen käsittely oli myös oma haasteensa. Työarkkeja kertyi lopulta yli 800 ja niiden manuaalinen läpikäynti oli raskas

ja aikaa vievä prosessi. Avointen vastausten analysoiminen ja tulosten muovaaminen esitettävään muotoon ei onnistunut käden käänteessä.

Henkilöstön tietoturvatyöpajojen järjestäminen oli täynnä haasteita, joista osa oli odotettuja ja osa tuli yllätyksenä. Tarvittavat työpajat saatiin kuitenkin järjestettyä ja tulokset esitettyä toivotulla tavalla, mutta kaikki tämä vaati paljon työtä.

8.3 Työpajojen toimivuus tietoturvakoulutuksessa ja -arvioinnissa

Tietoturvatyötyöskentely oli kokonaisuutena toimiva tapa kouluttaa yrityksen henkilökuntaa toimimaan tietoturvallisemmin ja oppimaan tietoturva-asioita. Henkilöstön tietoturvakouluttaminen perinteisistä koulutustavoista poikkeavin menetelmin osoittautui mielekkääksi ja toimivaksi sekä näin järjestäjän että kohdeyleisön mielestä. Työpajatyöskentelyssä luennointi jätettiin vähäiseksi ja aiheesta voitiin keskustella avoimesti. Lisäksi yleisö sai esittää vapaasti kysymyksiä aiheesta ja pohtia tietoturvaa sekä itsenäisten että ryhmässä tehtävien työvaiheiden avulla.

Työpajojen käyttö tietoturvaheikkouksien tai parannuskohteiden etsimiseen ei sekään ollut kaikkein perinteisin tapa toimia. Yleensä mittaukset suoritetaan suljetuin kyselyin, jotka lähetetään sähköisesti suoraan kohdeyleisölle. Tietoturvatyöpajoissa käytetyt työarkit toimivat sekä avoimina vastauslomakkeina että harjoitteina, ja ne tuottivat suuren määrän henkilöstön tietoturvalliseen toimintaan liittyviä parannuskohteita.

Työpajojen hyvästä toimivuudesta huolimatta on huomioitava, että työarkkien hyödyntäminen ei ole kyselymuotoisena mittaamismenetelmänä täysin aukoton. Syynä tähän on se, että osallistujat pohtivat itsenäisesti esimerkkejä työarkkeihin. Tämän seurauksena yksittäiset työntekijät eivät välttämättä halunneet kertoa niistä omista tai osastonsa toimintatavoista, jotka eivät ole täysin tietoturvallisia. Lisäksi henkilöstön pohtimat parannuskohteet saattavat olla osittain tietoturvan yleisohjeiden tai yrityksen tietoturvakäytäntöjen kannalta virheellisiä. Työntekijät eivät välttämättä myöskään tunnistaneet virheellistä toimintaa, jolloin esimerkkejä ei tullut kirjatuksi lainkaan. Nämä havainnot on hyvä ottaa huomioon tämän tutkimuksen tuloksiin perustuvissa jatkotoimenpiteissä.

8.4 Kokonaiskuva

Suuri, haastava, työläs ja palkitseva ovat sanoja, joilla voisi kuvailla tietoturvatyöpajojen kokonaisvaltaista hyödyntämistä suuren yrityksen tietoturvakehityksessä. Suuren henkilöstömäärän ja aineiston käsittely oli haastavaa ja työlästä. Haasteita riitti alusta loppuun asti, mutta niihin löydettiin tehokkaasti ratkaisut ja kaikkiin tavoitteisiin päästiin.

Tietoturvatyöpajojen järjestäminen ja niistä kerätyn aineiston analysointi olivat itselleni opettava kokemus. Koen, että koulutuksien ja eri tilaisuuksien järjestäminen on jatkossa itselleni huomattavasti helpompaa. Lisäksi huomasin kehittyväni asioiden organisoinnissa, ajanhallinnassa ja ongelmanratkaisussa koko työpajaprosessin ajan. Mikäli saisin palata koko prosessin alkuun, en tekisi haasteista ja suuresta työmäärästä huolimatta mitään toisin.

Loppujen lopuksi tietoturvatyöpajojen kokonaisvaltainen hyödyntäminen on palkitsevaa myös kohdeyritykselle. Kattavat tulokset pitävät sisällään paljon arvokasta tietoa, joka on hyödynnettävissä toimeksiantajan haluamalla tavalla. Vastaavanlaisia työpajoja voidaan hyödyntää kohdeyrityksen lisäksi myös muissa yrityksissä ja organisaatioissa korkeamman henkilöstö- ja kokonaistietoturvatason saavuttamiseksi.

LÄHTEET

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Andress, J. 2011. The Basics of Information Security. 1st Edition. Amsterdam: Syngress.

Bisson, D. 2015. 5 Social Engineering Attacks to Watch Out For. Tripwire. Viitattu 8.3.2016 http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.

Bond, T. 2012. Employee Security Awareness Survey. Viitattu 14.3.2016 https://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf.

Brook, D. & Sharma, R. 2016. People power: making your people an essential part of your cyber security strategy. PA Consulting Group. Viitattu 15.3.2016 http://www.paconsulting.com/our-thinking/why-a-human-side-is-essential-to-effective-cyber-security/.

City of Winnipeg's Audit Department. 2008. The Assessment of Information Security Awareness. Viitattu 17.3.2016 http://www.winnipeg.ca/audit/pdfs/reports/ITSecurityAwareness.pdf.

Commission for the Protection of Privacy. 2015. Non-repudiation (Information Security). Viitattu 23.12.2015 https://www.privacycommission.be/en/glossary/non-repudiation.

Copley, S. 2015. Data and Information. Viitattu 3.11.2015 http://www.igcseict.info/theory/0/data/.

Criddle, L. 2016. What is Social Engineering? Viitattu 6.3.2016 http://www.webroot.com/hk/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering.

Doyle, M. 2014. What is the Difference Between Data and Information? DQ Global. Viitattu 3.11.2015 http://www.dqglobal.com/2014/05/27/what-is-the-difference-between-data-and-information/.

Flat Iron Technologies. 2014. What is COBIT? | Control Objectives for Information and Related Technologies. Viitattu 12.4.2016 http://www.flatirontech.org/faq/what-is-cobit.

Henry, A. 2014. How Spammers Spoof Your Email Address (and How to Protect Yourself). Lifehacker. Viitattu 8.3.2016 http://lifehacker.com/how-spammers-spoof-your-email-address-and-how-to-prote-1579478914.

i&i Solutions. 2015. Tietoturva. Viitattu 26.2.2016 heikki.pp.fi/ijai/12.pdf.

IT Governance. 2016. The ISO/IEC 27000 Family of Information Security Standards. Viitattu 12.4.2016 http://www.itgovernance.co.uk/iso27000-family.aspx.

Iyengar, V. 2010. Information Security for Management. Mumbai: Himalaya Publishing House.

Järvinen, P. 2012. Arjen tietoturva: vinkit & ratkaisut. Jyväskylä: Docendo.

Laaksonen, M.; Nevasalo, T. & Tomula K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Lacey, D. 2009. Managing the Human Factor in Information Security. How to win over staff and influence business managers. Chichester: Wiley.

National Institute of Electronics and Information Technology. 2015. Report on One Day Workshop on Cyber Security Awareness. Viitattu 18.3.2016 http://imphal.nielit.gov.in/wp/wp-content/uploads/2015/02/Report-on-cyber-security-awareness-workshop-24-02-2015.pdf.

Oikarinen, T. 2012. Tietoturvallisuus julkisessa hallinnossa. Sähköisen hallinnon perusteet. Viitattu 26.2.2016 http://wanda.uef.fi/oikeustieteet/luennot12-13/Tietoturva-2012-12-13.pdf.

Penttinen, P. 2015. Joensuun kaupungin tietoturvapolitiikka. Viitattu 25.2.2016 http://webdynasty.jns.fi/djulkaisu/kokous/2015638-5-2.PDF.

Perrin, C. 2008. The CIA Triad. TechRepublic. Viitattu 4.11.2015 http://www.techrepublic.com/blog/it-security/the-cia-triad/.

Rousku. K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

SANS Institute. 2001. The Weakest Link: The Human Factor Lessons Learned from the German WWII Enigma Cryptosystem. Viitattu 4.3.2016 https://www.giac.org/paper/gsec/792/security-awareness-preventing-lack-security-consciousness/101700.

Shinder, D. 2013a. Security Awareness Training: Your First Line of Defense (Part 1). WindowSecurity. Viitattu 16.3.2016 http://www.windowsecurity.com/articles-tutorials/misc_network_security/security-awareness-training-your-first-line-defense-part1.html.

Shinder, D. 2013b. Security Awareness Training: Your First Line of Defense (Part 2). WindowSecurity. Viitattu 16.3.2016 http://www.windowsecurity.com/articles-tutorials/misc_network_security/security-awareness-training-your-first-line-defense-part2.html.

Sosiaali- ja terveysministeriö. 2007. Tietoturvallisuussuunnitelman laatiminen. Sosiaali- ja terveysministeriön julkaisuja 2007:19. Helsinki: Sosiaali- ja terveysministeriö. Saatavissa myös https://www.julkari.fi/bitstream/handle/10024/113147/julkaisuja_2007_19_tietoturvallisuussuunnitelma_verkko.pdf?sequence=1.

Suomen Kuntaliitto. 2016. Tietoturva. Viitattu 26.2.2016 http://www.kunnat.net/fi/asiantuntijapalvelut/tyk/tietohallinto/tietoturva/Sivut/default.aspx.

Tietosuojavaltuutetun toimisto. 2010. Pharming, mitä se on? Viitattu 7.3.2016 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq9mcbP/Pharming_mita_se_on.pdf.

Touhill, G. J. & Touhill, C. J. 2014. Cybersecurity for Executives: A Practical Guide. New Jersey: Wiley.

Valtiontalouden tarkastusvirasto. 2011. Valtionhallinnon tarkastusviraston toimintakäsikirja. Määräys tietoturvallisuudesta tarkastusvirastossa. Viitattu 26.2.2016 https://www.vtv.fi/files/2828/VTV_tietoturvamaarays_paivitys_lopullinen.pdf.

Valtiovarainministeriö. 2008a. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008. Helsinki: Edita Prima. Saatavissa myös https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10128&groupId=10229.

Valtiovarainministeriö. 2008b. Valtionhallinnon tietoturvasanasto, VAHTI 8/2008. Helsinki: Edita Prima. Saatavissa myös https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10128&groupId=10229.

Virginia Department for Aging and Rehabilitative Services. 2012. End User Cyber Security Awareness Training. Viitattu 17.3.2015 http://www.vda.virginia.gov/ppt/SecurityAwarenessTraining.pptx.

Voss, B. D. 2001. The Ultimate Defense of Depth: Security Awareness in Your Company. Viitattu 5.3.2016 http://www.sans.org/reading-room/whitepapers/awareness/ultimate-defense-depth-security-awareness-company-39.

Väistö, H. 2005. Hallinnollinen tietoturvallisuus. Viitattu 23.12.2015 http://www2.amk.fi/digma.fi/www.amk.fi/material/attachments/vanhaamk/etuotanto/041005/5h2DTrXIx/Hallinnollinen_tietoturva.pdf.

Liite 1: Turun tuotantolaitokselta osallistuvat osastot

Osaston nimi	Selite/suomennos	Työntekijöiden määrä
Accounting & Tax	Talousosasto	6
Chemical Laboratory	Kemiallinen laboratorio	44
Corporate Communication	Viestintäosasto	1
Corporate Controlling	Yritystoiminnan kontrollointiosasto	1
Demand Management & Transportation	Kysynnänhallinta ja kuljetukset	12
Facility Management – Production	Laitoshuollon tuotantotyöntekijät	11
Facility Management	Laitoshuollon toimihenkilöt	6
General Administration	Yleishallinto	2
Global Chemical and Pharmaceutical Development Finland – Analytical Development	Analyyttisen kehityksen osasto	30
Global Chemical and Pharmaceutical Development Finland – Polymer Technology & Formulation Development	Polymeeriteknologian ja -muotoilemisen kehitysosasto	26
Global Chemical and Pharmaceutical Development Finland – Quality Assurance	Tuotekehityksen laadunvarmistus	2
Global Chemical and Pharmaceutical Development Finland Common	Tuotekehityksen johto ja johdon avustajat	2
Global Chemical and Pharmaceutical Development Finland Operations	Tuotekehitystoimintojen osasto	4
Global Healthcare Programs	Globaali terveydenhuolto-ohjelmia hallinnoiva osasto	2

Health, Safety & Environment, HSE	Terveys-, turvallisuus- ja ympäristöasioiden hoito	4
Human Resources	Henkilöstöosasto	9
Implant Assembly – Production	Ihon alle asetettavan pienen muovisen ehkäisytuotteen eli implantaattituotteen kokoonpanotyöntekijät	109
IT Administration & Management	Hallinnollisten IT-asioiden hallintaosasto	3
IT Business Applications	Liiketoimintaohjelmistojen hallintaosasto	7
IT Operations & Infrastructure	IT-toimintojen ja -infrastruktuurin hallintaosasto	8
IUD (Intrauterine device) & Core – Production	Kierukka- ja hormoniydinvalmistuksen tuotantotyöntekijät	12
IUD Assembly – Production	Kohdunsisäisen ehkäisytuotteen eli kierukkatuotteen kokoonpanotyöntekijät	57
Law, Patents & Compliance	Laki- ja patenttiosasto	8
Layout & Labelling Management	Ulkoasun ja etiketöinnin hallinta	6
Life Cycle Management	Tuote- ja prosessielinkaarien hallintaosasto	16
Machinery – Production	Korjaamon ja laitehuollon tuotantotyöntekijät	6
Machinery	Tuotantokoneiden ja -laitteistojen ylläpidon toimihenkilöt	9
Main Production Supervisors	Kierukka-, implantaatti- ja IUD-osastojen työnjohto	13
Medical Affairs	Lääketeollisuuden toimintoja tukeva osasto	1

Microbiological Laboratory	Mikrobiologinen laboratorio	16
Occupational Health Care	Työterveyshuolto	5
Operational Excellence	Toiminnan kehittämisosasto	5
Pharmacovigilance	Lääketurvallisuusosasto	2
Procurement	Hankintaosasto	6
Product Supply	Tuotantolaitoksen johto ja johdon avustajat	7
Production Management & Experts	Tuotantopäälliköt ja tuotannon asiantuntijat	11
Production Planning & Master Data	Tuotannon suunnittelu ja Master Datan eli liiketoiminnan kannalta tärkeän tiedon hallinta	6
Quality & Compliance	Laadunhallinta	10
Quality Assurance	Laadunvarmistusosasto	17
Quality Management & HSE Common	Laadunhallinnan ja HSE:n johto avustajineen	3
Research & Development Controlling	Tuotekehityksen ja -tutkimuksen kontrollointi	2
Security, Energy & Engineering	Turvallisuus, energia ja tekniikka	3
Site Services	Tuotantolaitoksen sisäiset palvelut	11
Solids Forms Production & Packaging – Production	Tablettivalmistuksen ja -pakkaamon tuotantotyöntekijät	27
Solids Forms Production & Packaging	Tablettivalmistuksen ja -pakkaamon työnjohto	6
Study Management	Tutkimuksen hallinnointiosasto	1
Supply Chain Management Director & Coordinator	Toimitusketjujen ja logistiikan hallinnan johtaja ja koordinoija	2
Validation	Validointiosasto	8
Warehouse Management – Production	Varastojen ja lähettämön tuotantotyöntekijät	14
Warehouse Management	Varastojen ja lähettämön toimihenkilöt	4

Women’s Healthcare Mixing & Extrusions – Production	Materiaalivalmistuksen tuotantotyöntekijät	16
Women’s Healthcare Mixing & Extrusions	Materiaalien valmistusosaston työnjohto	3
Women's Healthcare Packaging – Production	Ehkäisyvälinepakkaamon tuotantotyöntekijät	30
Women's Healthcare Packaging	Ehkäisyvälinepakkaamon työnjohto	4

Liite 2: Espoon toimipisteestä osallistuvat yrityksen omat osastot

Osaston nimi	Selite/suomennos	Työntekijöiden määrä
BU General Medicine	Yleislääkeosasto	3
BU Specialty Medicine	Erikoislääkeosasto	2
BU Women's Healthcare	Naisterveydenhuollon asiantuntijat	2
Business Support	Liiketoiminnan tukiosasto	5
Business Support Marketing Services	Liiketoiminnan tuen markkinointipalvelut	3
Clinical Project Management Specialty Medicine Oncology I	Kliinisten projektien hallinnan ja erikoislääkkeiden onkologian osasto	5
Consumer Care Regulatory Affairs	Asiakaspalvelua säätelevä osasto	1
Corporate Communication	Viestintäosasto	1
Corporate Controlling	Yritystoiminnan kontrollointios-asto	1
Crop Science	Kasvinsuojeluosasto	4
Crop Science Environmental Science	Tuhoeläinten ja rikkakasvien torjunnan erikoisosasto	1
Global Clinical Development Operations Finland	Globaalin kliinisen kehityksen osasto	9
Global Clinical Development Operations Quality & Compliance	Globaalin kliinisen kehityksen laadunhallintaosasto	2
Global Data Sciences & Analytics	Globaalin datatutkimuksen osasto	2
Global Site Management	Toimipistehallinnoinnin osasto	13
Human Resources	Henkilöstöosasto	2
Law, Patents & Compliance	Laki- ja patenttiosasto	2
Market Access	Markkinoillepääsyä hoitava osasto	3

Medical & Regulatory Affairs	Lääketeollisuuden toimintoja sekä lääkemääräysten ja -säännösten mukaista toimintaa ylläpitävä osasto	2
Medical Affairs	Lääketeollisuuden toimintoja tukeva osasto	5
Medical Writing	Lääketieteellisen kirjoittamisen osasto	5
Pharmaceutical Controlling	Lääkekontrolloinnin osasto	4
Pharmaceuticals Finland	Reseptilääkkeistä vastaava osasto	2
Pharmacovigilance	Lääketurvaosasto	2
Procurement	Hankintaosasto	2
Regulatory Affairs	Lääkemääräysten ja -säännösten mukaista toimintaa ylläpitävä osasto	5
Samson Special Items	Samson-erikoisyksikkö	1

Liite 3: Muut osallistuvat osastot

Espoon toimipisteen vuokratyöntekijäosastot

Osaston nimi	Selite/suomennos	Työntekijöiden määrä
Clinical Project Management Specialty Medicine Oncology I	Kliinisten projektien hallinnan ja erikoislääkkeiden onkologian osasto	10
Global Clinical Development Operations Finland	Kliinisen kehityksen osasto	10
Global Medical Writing	Globaalin lääketieteellisen kirjoittamisen osasto	7
Global Site Management	Toimipistehallinnoinnin osasto	22

Myyntihenkilöstö

Osaston nimi	Selite/suomennos	Työntekijöiden määrä
Women’s Healthcare Sales	Ehkäisyvälineiden myynnistä vastaava ryhmä	5

Liite 4: Tietoturvatyöpajojen työarkit

Työarkki 1

Osasto: _____ Työpajaryhmä: _____ Päivämäärä: _____

Mihin kaikkeen arvokkaaseen informaatioon ja dataan sinulla on pääsy? ➔ Työarkki 1

Työskentele itsenäisesti:

Luo lista kaikesta arvokkaasta informaatiosta ja datasta, johon sinulla on pääsy ja joka voisi vääriin käsiin joutuessaan vahingoittaa yritystä.

Käytä saamaasi paperia – sinulla on aikaa 10 MIN

Pohdi niin monta esimerkkiä kuin mahdollista. Jokaisen panos on tärkeä!

Työarkki 2

Osasto: _____ Työpajaryhmä: _____ Päivämäärä: _____

Miten sinä voit tehdä yrityksestä tietoturvallisemman? ➔ Työarkki 2

Työskentele itsenäisesti:

Missä asioissa olisi kehitettävää?

Listaa heikkouksien pohjalta ideasi siitä, kuinka sinä ja tiimisi voivat tehdä organisaatiostamme tietoturvallisemman.

Esimerkiksi:

Miten käyttäytymisemme tulisi muuttua?

Miten prosessiemme tulisi muuttua?

Muistitikut, salasanat, tiedon jakaminen ulkopuolisille, sosiaalinen media…

Käytä saamaasi paperia – sinulla on aikaa **10 MIN**

_____

_____

_____

_____

_____

_____

_____

Palaute (lopuksi ennen työpajasta poistumista)	Täysin samaa mieltä	Osittain samaa mieltä	Eri mieltä
Tämä tietoturvatyöpaja lisäsi tietoturvatietoisuutta työpajaryhmässäni.			
Tämä työpaja on ollut hyödyllinen ajatellen osastoni/tiimini tietoturvatason nostamista.			
Meillä on kysymyksiä tai tarvitsemme apua tietyissä tietoturvaan liittyvissä asioissa. Olkaa hyvä ja ottakaa meihin/minuun yhteyttä. *			

* Kirjoita nimesi yhteydenottoa varten, mikäli merkitsit rastin alimpaan kohtaan.

Nimi: _____